Air Live®
Powered by OvisLink Corp.

WH-9200AP

802.11a/b/g Dual Radio Wireless Base Station

User's Manual





Copyright & Disclaimer

No part of this publication may be reproduced in any form or by any means, whether electronic, mechanical, photocopying, or recording without the written consent of OvisLink Corp.

OvisLink Corp. has made the best effort to ensure the accuracy of the information in this user's guide. However, we are not liable for the inaccuracies or errors in this guide. Please use with caution. All information is subject to change without notice

All Trademarks are properties of their respective holders.

Regulatory Information

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, (example - use only shielded interface cables when connecting to computer or peripheral devices) any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For product available in the USA/Canada market, only channel 1~11 can be operated.

Selection of other channels is not possible.

IMPORTANT NOTE

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC NOTICE: To comply with FCC part 15 rules in the United States, the system must be professionally installed to ensure compliance with the Part 15 certification. It is the responsibility of the operator and professional installer to ensure that only certified systems are deployed in the United States. The use of the system in any other combination (such as co-located antennas transmitting the same information) is expressly forbidden.

© 2009 OvisLink Corporation, All Rights Reserved

Table of Contents

1. Introduction 3

1.1 Overview 3

1.2 Installing WH-9200AP 4

1.2.1 Package Content 4
1.2.2 Hardware Presentation 4
1.2.3 Configuration Setups 8

2. Operation Mode of WH-9200AP 10

2.1 Change Operation Mode 10

2.2 Dual AP Mode 11

2.3 Duplex Mode 13

2.4 Dual WDS Bridge Mode 15

2.5 Separate Bridge Mode 17

2.6 AP + Client / Client + AP Mode 18

2.7 AP + WDS Bridge / WDS Bridge + AP Mode 20

2.8 WDS + Gateway / Gateway + WDS Mode 22

2.9 AP + Gateway / Gateway + AP Mode 24

2.10 AP + WISP / WISP + AP Mode 26

3. Wireless Settings 29

3.1 Access Point Mode 29

3.2 WDS Bridge Mode 30

3.3 Client Mode 32

3.4 Gateway (AP Router) Mode 35

3.4.1 WAN Port Settings 37
3.4.2 DHCP Server Settings 39
3.4.3 DMZ & Virtual Server 40
3.4.4 IP Filter Settings 41
3.4.5 IP Routing Settings 42
3.4.6 Dynamic DNS (DDNS) Settings 44

3.5 WISP Mode 45

3.6 Wireless Security 47

3.7 Advanced Wireless Settings 54

3.8 Access Control 57

3.9 Bandwidth Control.....59
3.9.1 Total Bandwidth Control.....60
3.9.2 Per user Bandwidth Control.....61
3.10 Multiple SSID + VLAN.....63
4. System Management 64
4.1 Change Password 64
4.2 System Management Settings.....65
4.3 SNMP Settings.....66
4.4 Firmware Upgrade 68
4.5 Configuration Save and Restore.....69
4.6 Reboot System 70
4.7 WH-9200AP Emergency Recovery.....70
5. Specifications.....72
6. Wireless Network Glossary.....76

1 Introduction

1.1 Overview

The WH-9200AP is a dream device for WISP to build their wireless networks. The AP features 2 Atheros 11a/b/g radios that run in 5GHz or 2.4GHz frequency band. Moreover, it provides hi-power at 11a mode for extra long distance application. There is an intergraded 802.3af POE port to let you run the AP at up to 100 meter distance away from the power source.

Dual Wireless + Hi Power + 2 LAN Ports

The WH-9200AP is equipped with 2 high-powered Atheros radios. The radio 1 runs in the 11a 5GHz mode only while the radio 2 runs at the 11a/b/g dual band mode. AirLive adds high power amplifier to run the AP at 23dBm in 11a mode (200mW), that's 4 times the output power of normal 11a radio (50mW). In addition, 2 programmable LAN ports are available for multi-mode AP/Gateway configuration.

Multiple Operation Modes

The WH-9200AP can operate in multiple wireless modes for different application environments such as Dual AP, Dual WDS, Duplex link aggregation, Separate Bridge, AP + Client, AP + WDS, WDS + Gateway, AP + Gateway, and AP + WISP. These modes can be changed and configured easily by the Web user interface.

802.3af PoE Port

WH-9200AP is equipped with an 802.3af Power over Ethernet port. It thus can be powered by a PoE PSE and operate at up to 100 meter away.

VLAN & QoS

WH-9200AP provides Multi-SSID to create different wireless networks using one AP. The TAG VLAN feature allows service provider to control service content of each SSID network all the way back to core router. The QoS feature allows prioritizing the different package according the 802.11e WMM protocol and triple play (Voice, Video and Data). Bandwidth control feature allow WH-9200AP to limit the bandwidth on distinct IP/MAC or on the total device.

IP67 Environmental Protection Enclosure

With IP-67 industrial standard enclosure, WH-9200AP is highly protected against dust and water. So that WH-9200AP can be used in a hardened environment.

1.2 Installing WH-9200AP

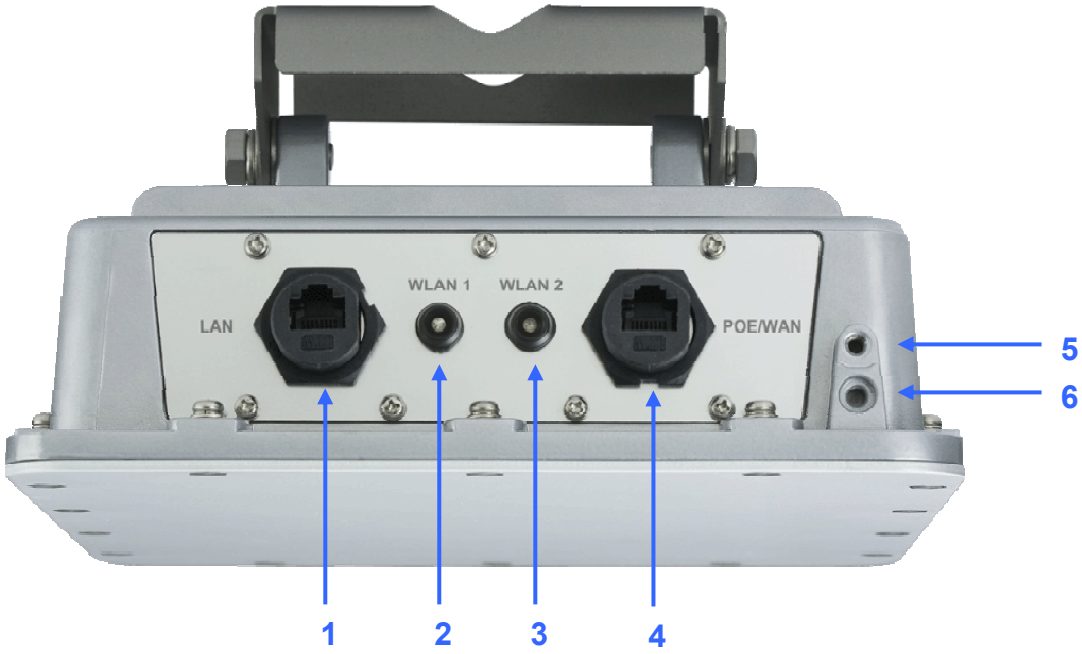
This section describes the installation procedure for the WH-9200AP. It starts with a summary of the content of the package you have purchased, followed by steps of how to power up and connect the WH-9200AP. Finally, this section explains how to configure a Windows PC to communicate with the WH-9200AP.

1.2.1 Package Content

The WH-9200AP package contains the following items:

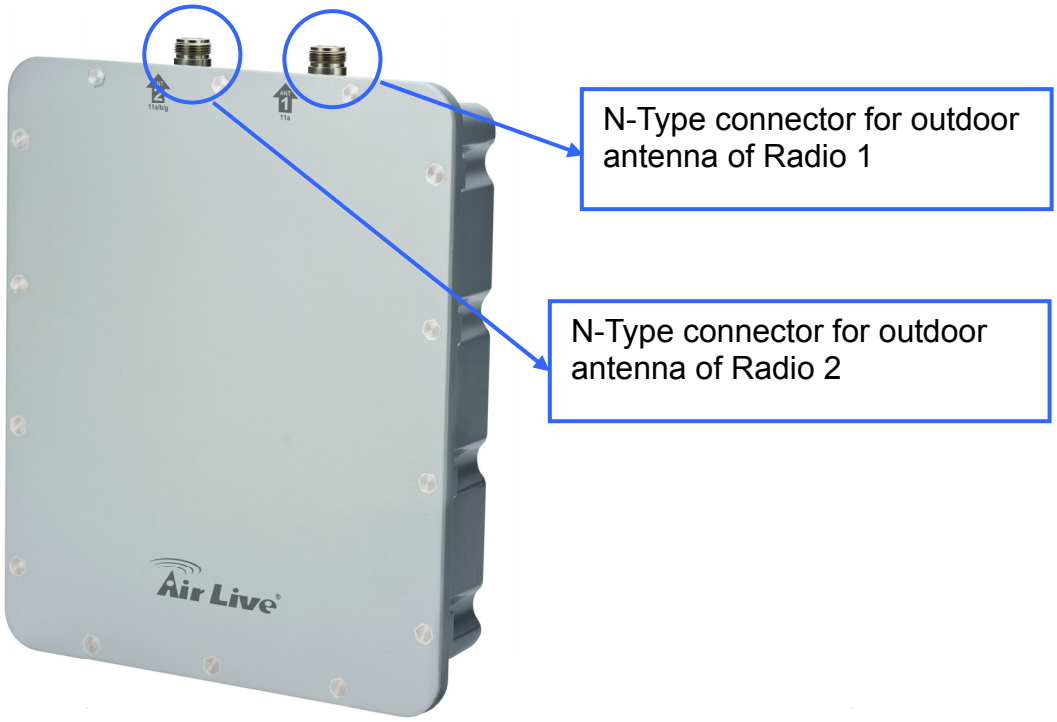
- One WH-9200AP main unit
- 48VDC PoE injector kits
- Pole/Wall mount kit
- One CD of the WH-9200AP
- Quick Start Guide

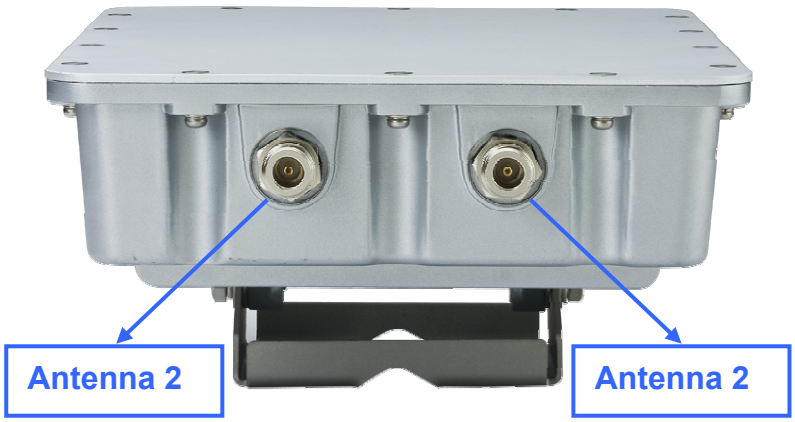
1.2.2 Hardware Presentation



LED #	Function	Color	Description
1	LAN	-	LAN port #2
2	WLAN1 LED	Blue	No Connection: Off

3	WLAN2 LED	Green	Low Signal: Flash per second Better Signal: Flash every 2 seconds Best Signal: Steady On
4	POE/WAN	-	LAN port #1, compatible with 802.3af PoE. Become WLAN port when operate in Gateway mode
5	Ground Pin	-	Reference point for electric current
6	Sluice	-	Sluice out the water in device

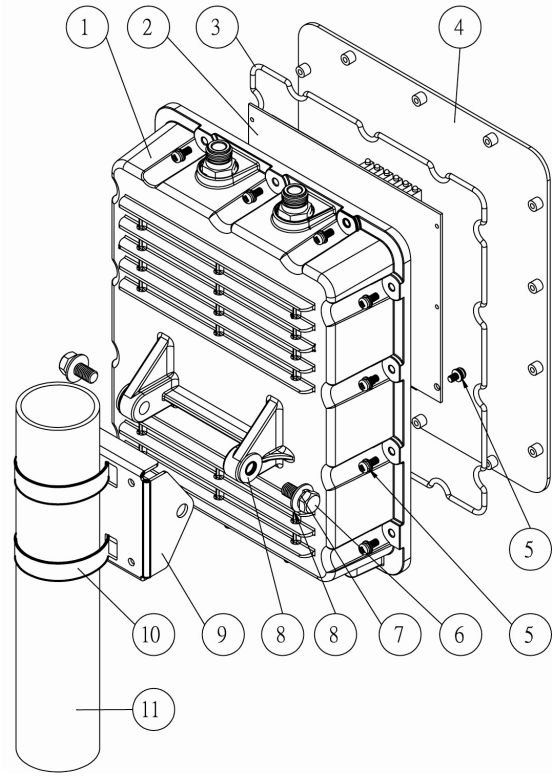




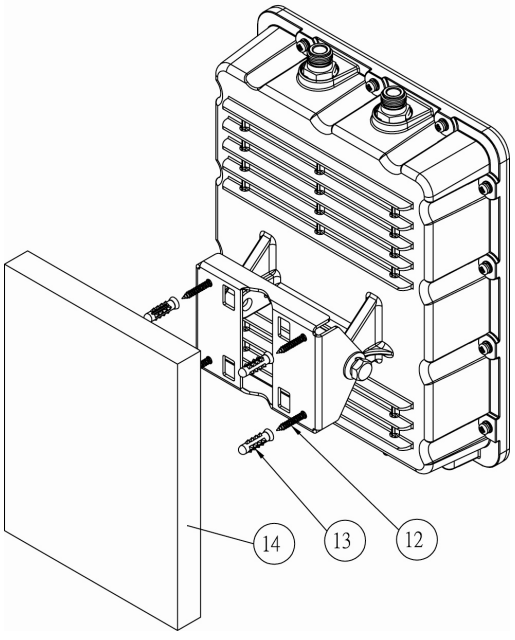
Pole Mount/Wall mount Installation

①	Enclosure assembly	- 1 set
②	PCB assembly	- 1 set
③	Gasket of front cover	- 1 pc
④	Front cover	- 1 pc
⑤	M4-10 screw	- 16 pcs
⑥	M8-20 screw	- 2 pcs
⑦	M8 spring washer	- 2 pcs
⑧	M8 washer	- 4 pcs
⑨	Mounting	- 1 pc
⑩	Pole clamp	- 2 pcs
⑪	POLE(MAX.:2 inch)	
⑫	Wall screw	- 4 pcs
⑬	Plastic anchor	- 4 pcs
⑭	Wall	

Pole Mount

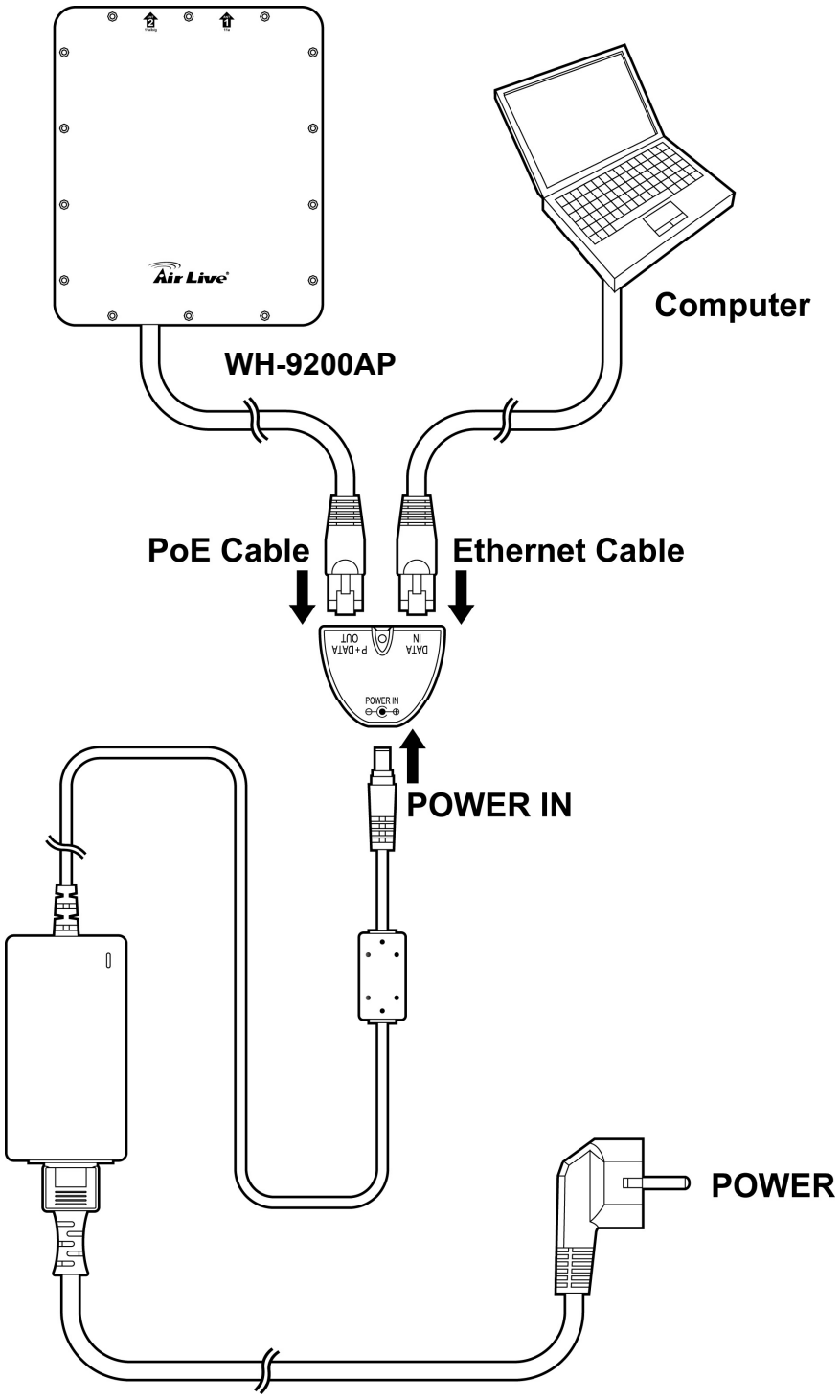


Wall Mount



Power Installation

The following image shows the power installation of WH-9200AP. Note that WH-9200AP is IEEE802.3af compatible, you should use the packed POE kit or POE Switch for power injection.



1.2.3 Configuration Setups

The factory default settings of WH-9200AP are as following:

Settings	Default Value	
	Wireless1	**Wireless2**
Device Name	WH-9200AP	
Radio	802.11a	802.11a
SSID	airlive1	airlive2
Channel	36	36 (auto in 802.11b/g)
WEP	Disabled	
IP Address	192.168.1.1	
DHCP Server	Disabled. Available and default enabled when each of the wireless is configured as a gateway.	
DHCP IP Range	192.168.1.2 ~ 192.168.1.254	
Access Password	airlive	

Note: Before you starting hardware connection, you are advised to find an appropriate location to place the Access Point. Usually, the best place for the Access Point is at the center of your wireless network, with line of straight to all your wireless stations. Also, remember to adjust the antenna; usually the higher the antenna is placed; the better will be the performance.

1. Connect to your local area network: connect an Ethernet cable to one of the Ethernet port.
2. (LAN1, LAN2) of this Wireless Access Point, and the other end to a hub, switch, router, or another wireless access point.
3. Power on the device: connect the included AC power adapter to the Wireless Access Point's power port and the other end to a wall outlet.

Access to management interface

1 Please make sure your computer IP is in the same subnet as the AP (i.e. 192.168.1.x).

2 Please make sure your computer has wireless network adapter installed.

3 Open the web browser and enter http://192.168.1.1/.



4. Connect Wireless Settings to start.

2 Operation Mode of WH-9200AP

The WH-9200AP device provides all 14 modes of wireless operational applications with:

Mode	Radio 1 (11a)	Radio 2 (11a/b/g)
Dual AP	Access Point	Access Point
Duplex	WDS Bridge	WDS Bridge
Dual WDS Bridge	WDS Bridge	WDS Bridge
Separate Bridge	WDS Bridge	WDS Bridge
AP + Client	Access Point	Wireless Client
Client + AP	Wireless Client	Access Point
AP + WDS Bridge	Access Point	WDS Bridge
WDS Bridge + AP	WDS Bridge	Access Point
WDS + Gateway	WDS Bridge	Gateway (AP Router)
Gateway + WDS	Gateway (AP Router)	WDS Bridge
AP + Gateway	Access Point	Gateway (AP Router)
Gateway + AP	Gateway (AP Router)	Access Point
AP + WISP	AP Router	WISP Bridge
WISP + AP	WISP mode	AP Router

2.1 Change Operation Mode

WH-9200AP is default in Dual AP mode. If the mode had been changed, click the **"Operation Mode"** button to change back.

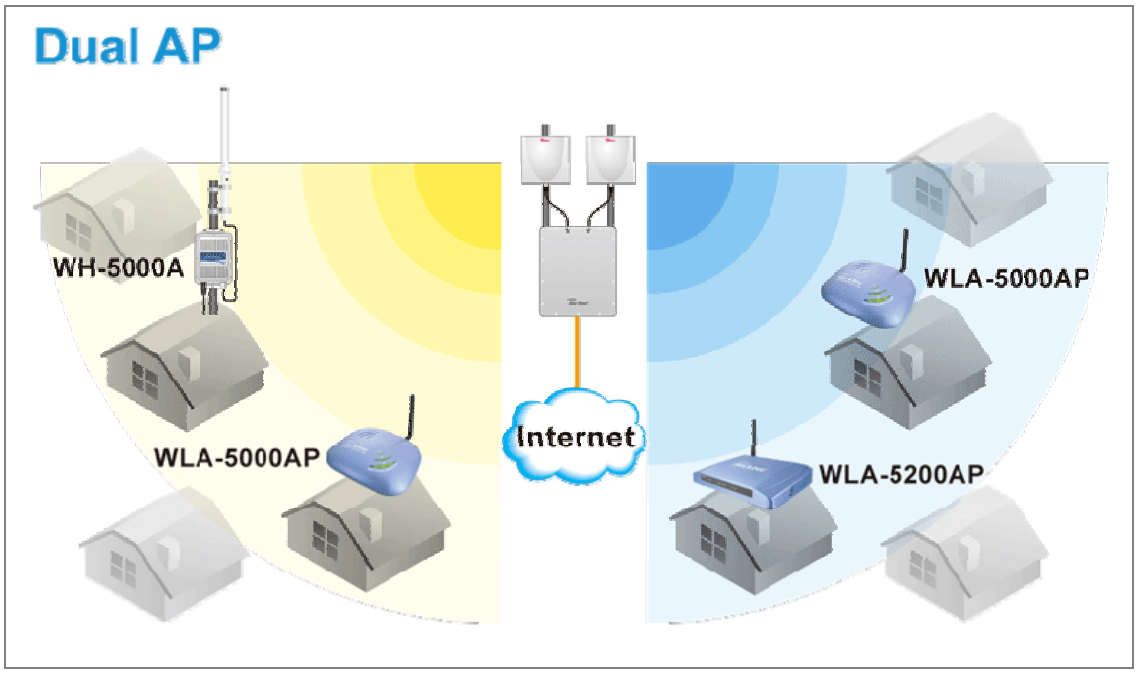
To change operation Mode:

1. Click on **"Operation Mode"**
2. Select Operation Mode in the main page
3. Click "Change Mode" button to apply
4. The device reboots to select mode

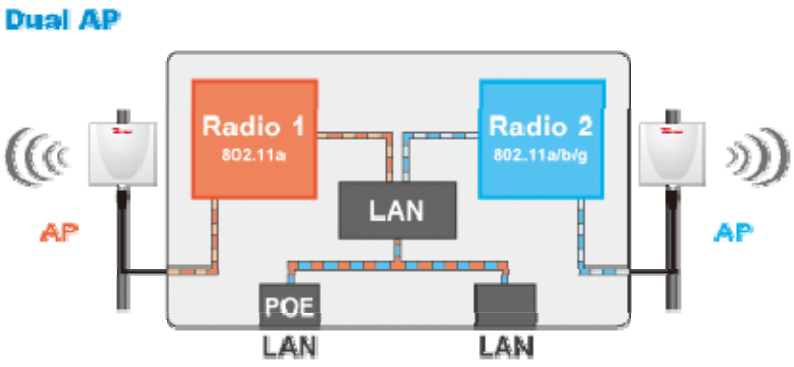


2.2 Dual AP Mode

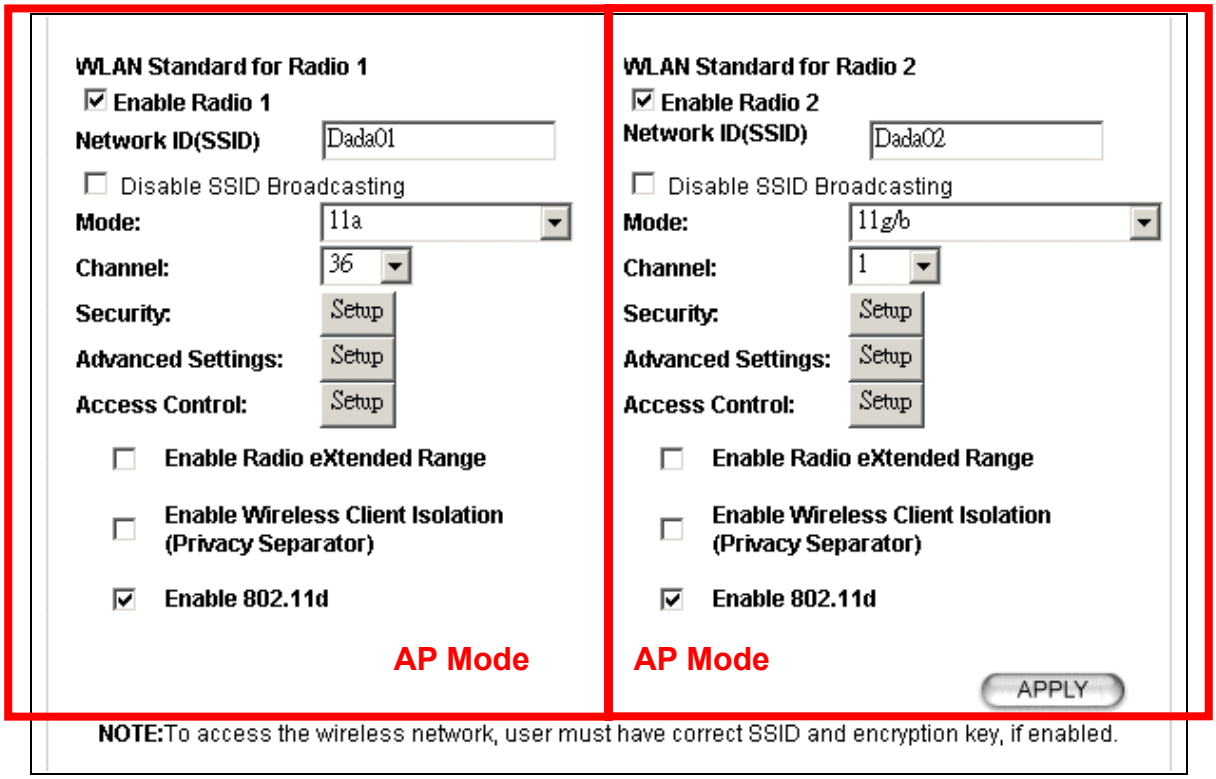
In Dual AP mode, both wireless interface of WH-9200AP are set as AP and provide hotspot service on each interface.



- This Application provides wider coverage that difficult to be reached with a unique Omni antenna by using another adequate antenna such as sector antenna. It's particularly suitable for WISP to provide stable and high performance link.
- The image in Dual AP mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.



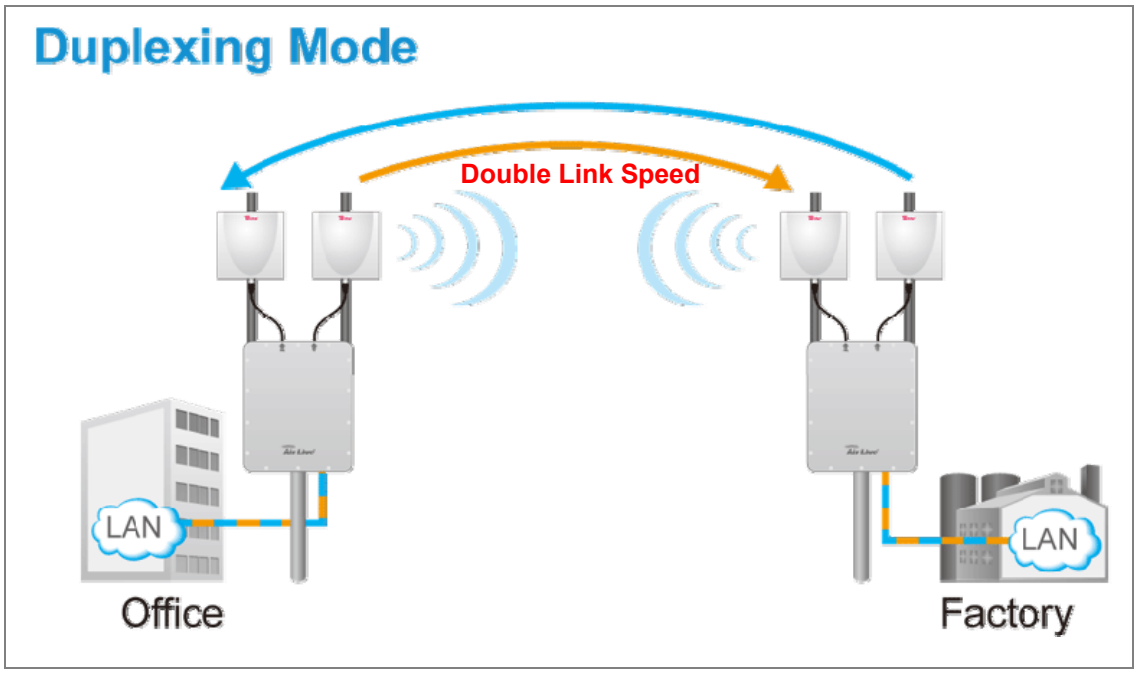
Both Radios has its own setting interface.



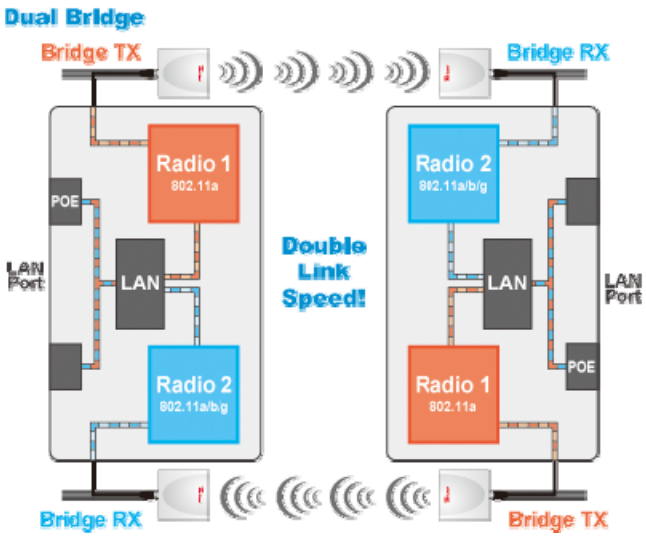
To configure AP mode, please refer to Section 3.1 Access Point Mode.

2.3 Duplex Mode

The duplex mode groups the two radios to double the bandwidth between two WH-9200APs.



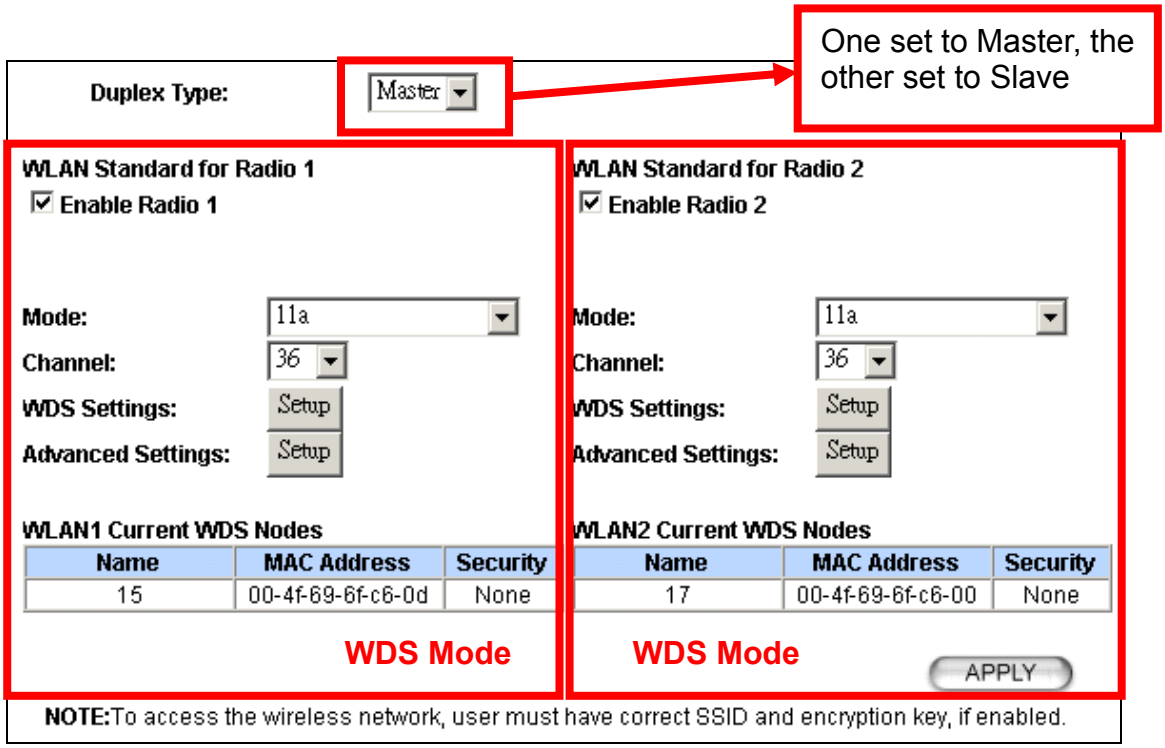
- This Application provides higher bandwidth between two locations than single radio does. When clients transmitting data which over the loading of single radio, the other radio shares the loading and make it able to transmit more data between the two WH-9200AP.



- The image in Duplex mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.

Both radios are using WDS mode for communication.

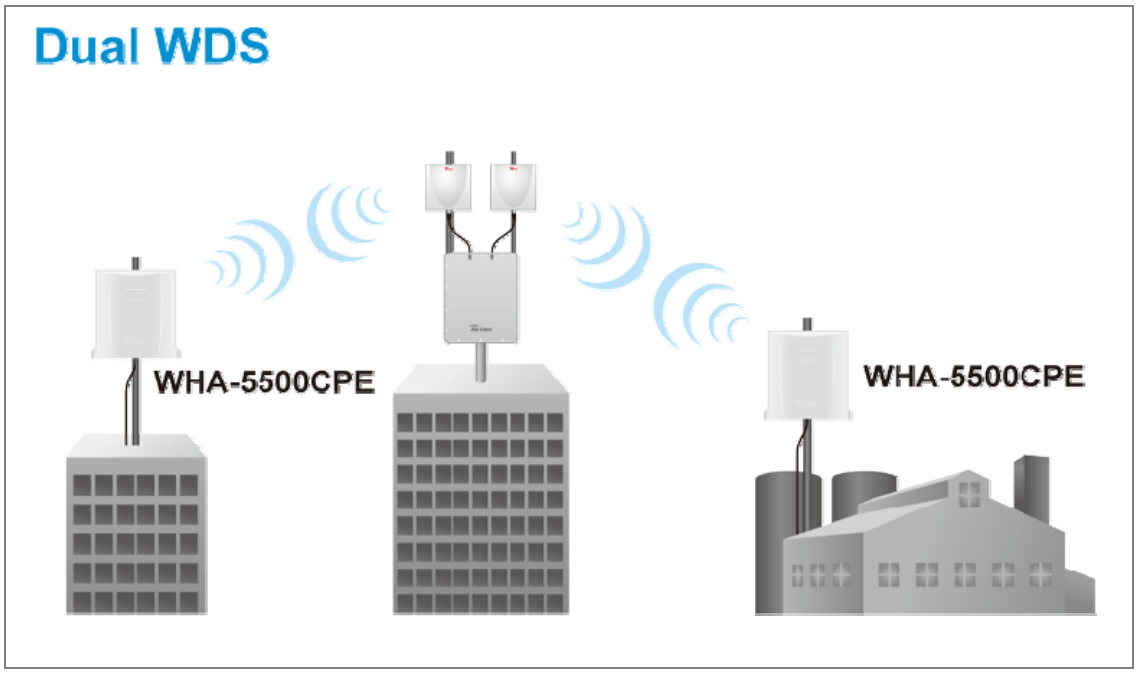
One WH-9200AP is configured as a Master where as the other WH-9200AP is configure to be a Slave.



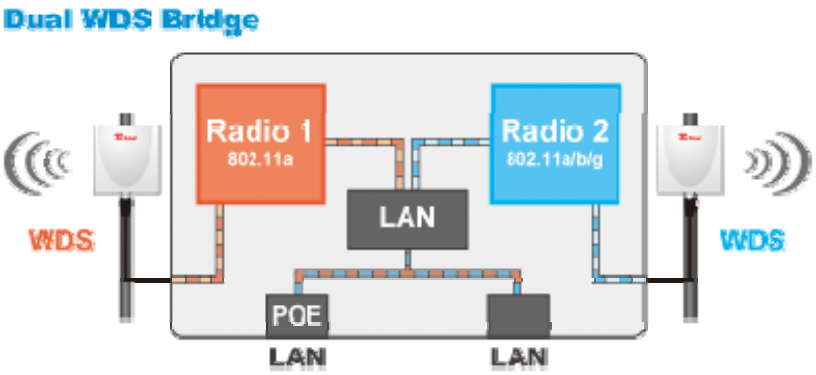
To configure the WDS mode, Please refer to Section 3.2 WDS Bridge Mode ……

2.4 Dual WDS Bridge Mode

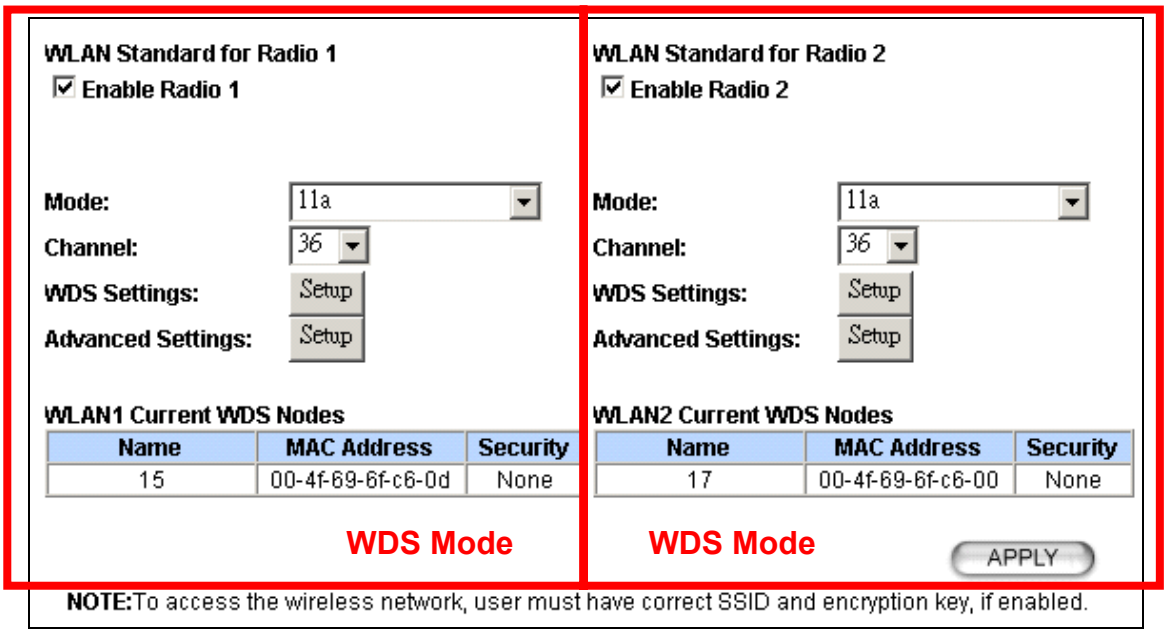
In Dual WDS Bridge mode, both wireless interface of WH-9200AP are set as WDS Bridge and connect to remote network. When configured in the Dual WDS Bridge mode, a WH-9200AP allows solving discontinuous link due to geographical obstacles, shown as below and extension of distance between two WDS bridge nodes separated by a building.



- In this mode, the AP can act as a signal repeating station in a wireless backbone network. In addition, it can also function as directing station for NLOS application.
- The image in Duplex WDS Bridge mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.



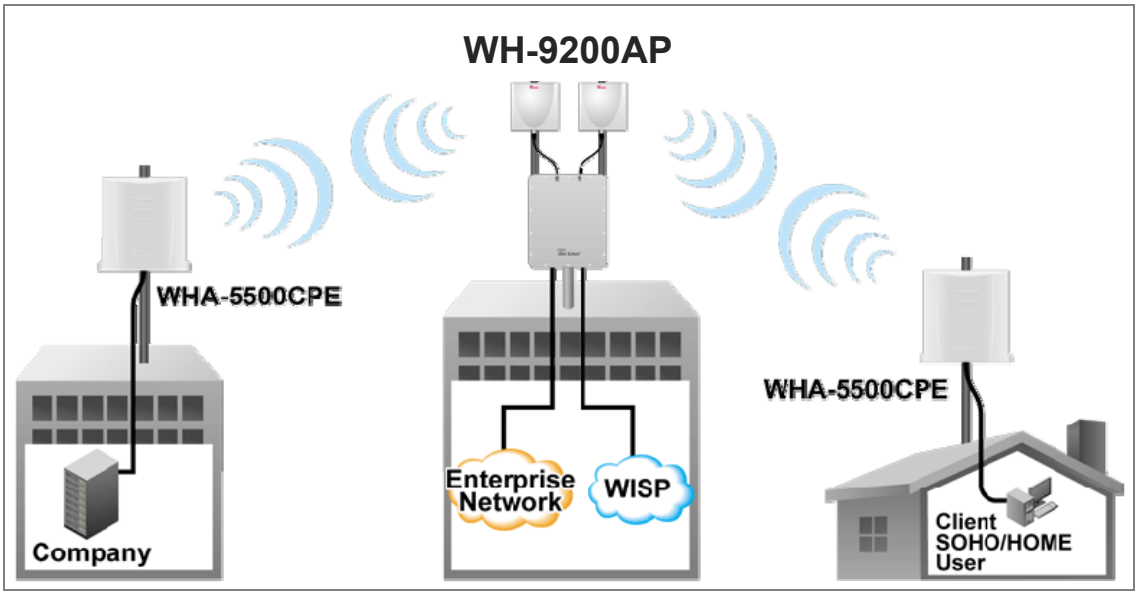
Both radios are using WDS mode for communication.



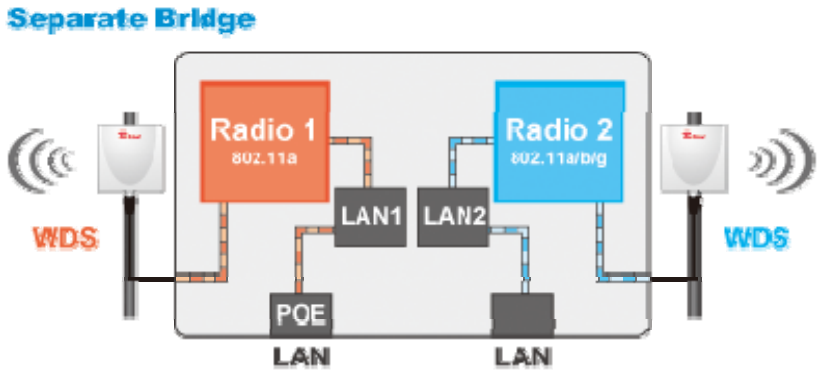
To configure the WDS mode please refer to section 3.2 WDS Bridge Mode ……

2.5 Separate Bridge Mode

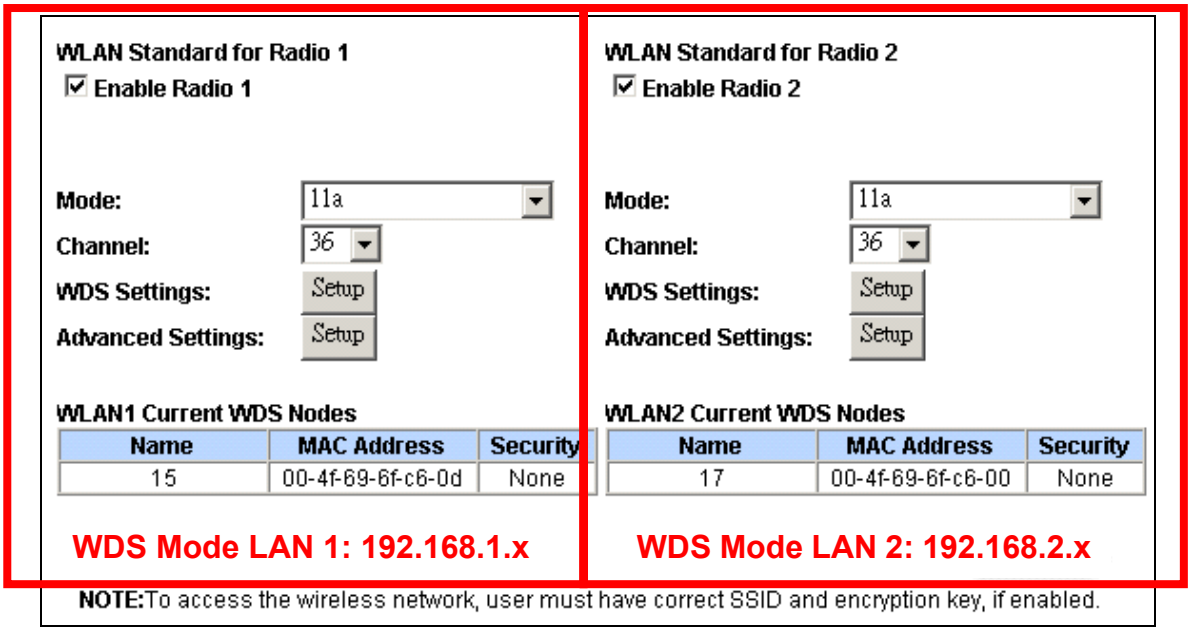
The Separate Bridge separates the device into 2 IP segments. Radio 1 and LAN 3 are in IP segment of 192.168.1.x/24 and Radio 2 and LAN1, LAN2 are in IP segment of 192.168.2.x. Devices in one IP segment can not communicate to devices in the other IP segment.



- In this application, both Radio 1 and Radio 2 are in WDS Bridge Mode.
- The image in Separate WDS Bridge mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.



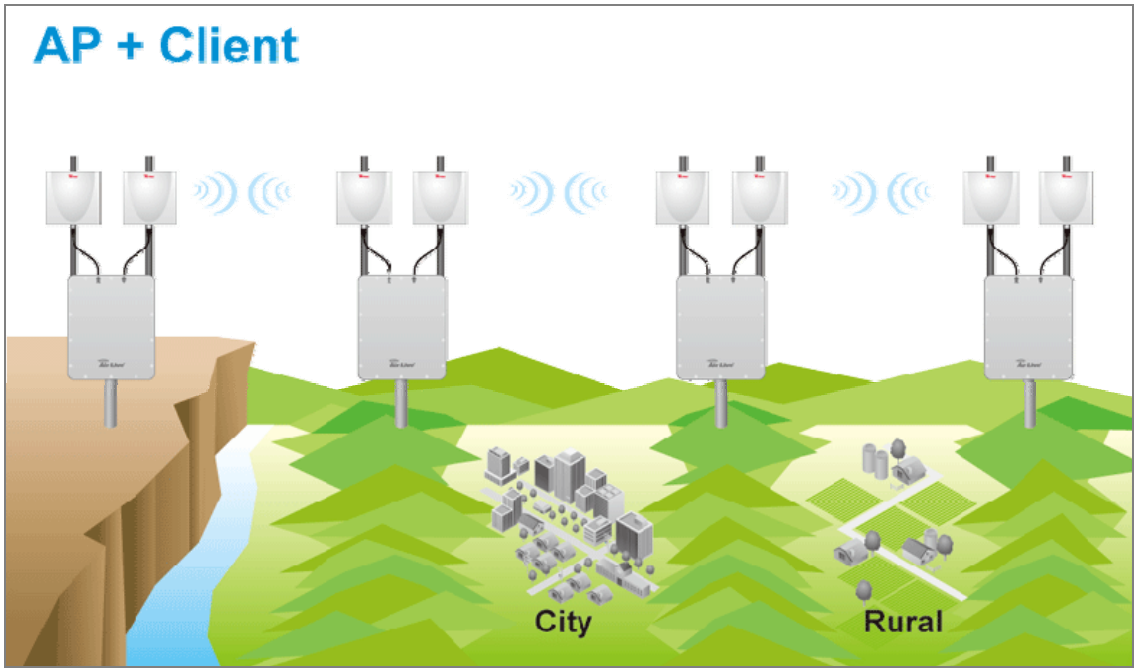
Both radios are using WDS mode for communication.



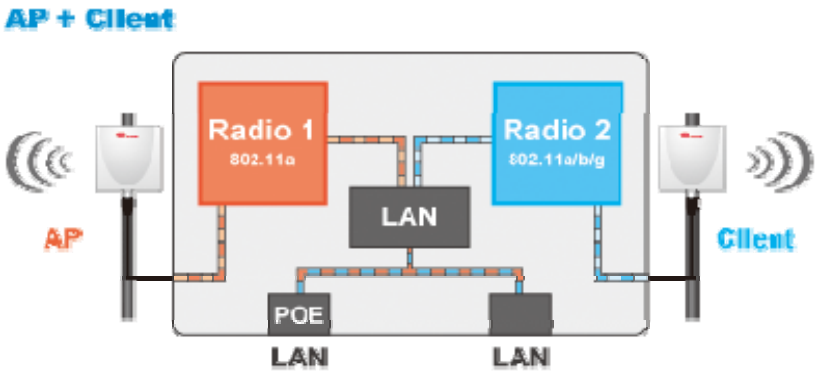
To configure the WDS mode, Please refer to Section 3.2 WDS Bridge Mode……

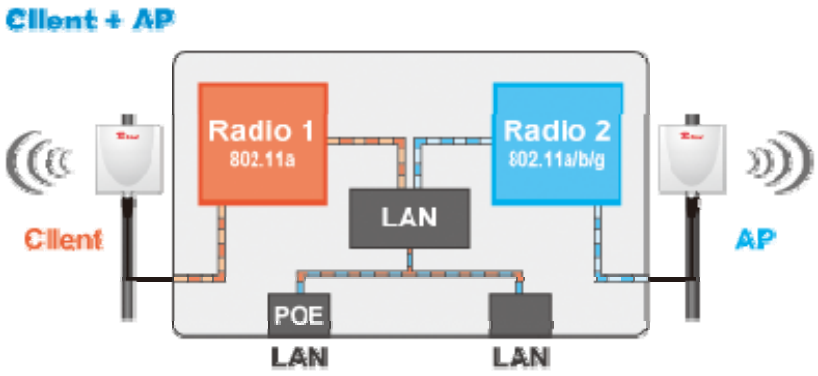
2.6 AP + Client / Client + AP Mode

In this mode, one station works as an intermediate station. This enable the AP to link with remote stations using client mode, then distribute the signal to other clients using AP mode.

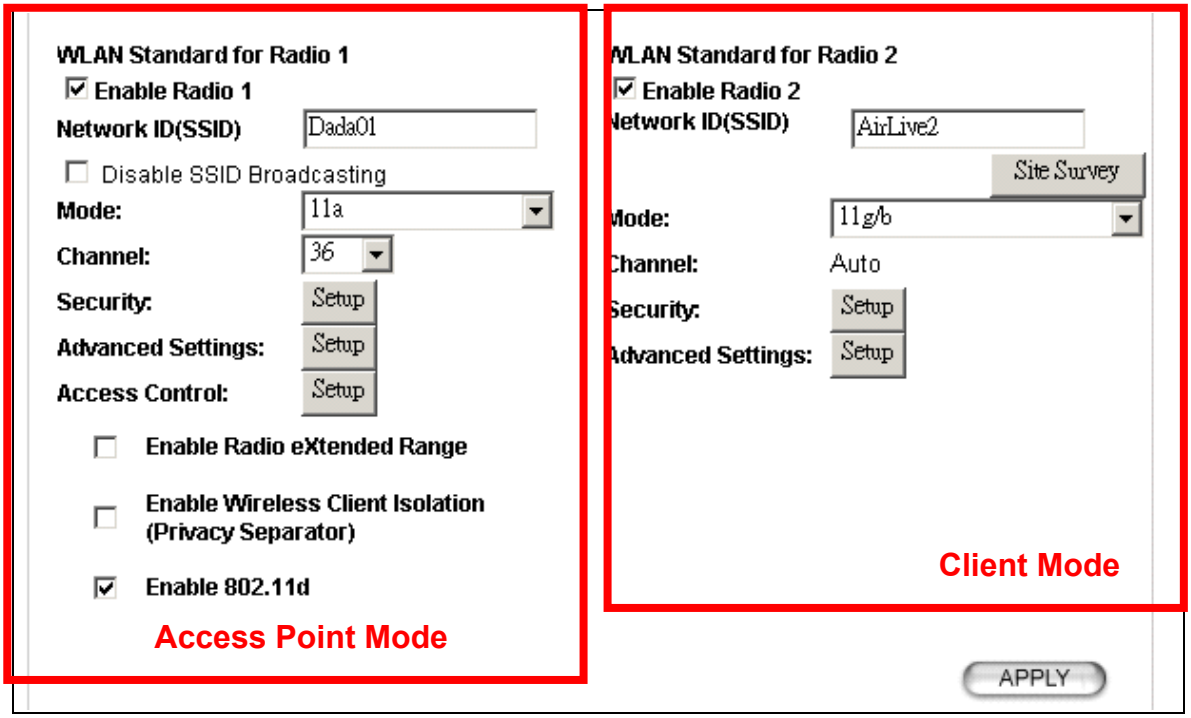


- In this application, Either Radio 1 or Radio 2 is in AP Mode, the other Radio is in Client mode.
- The image in AP + Client / Client + AP mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.





The UI example of AP + Client is as following:

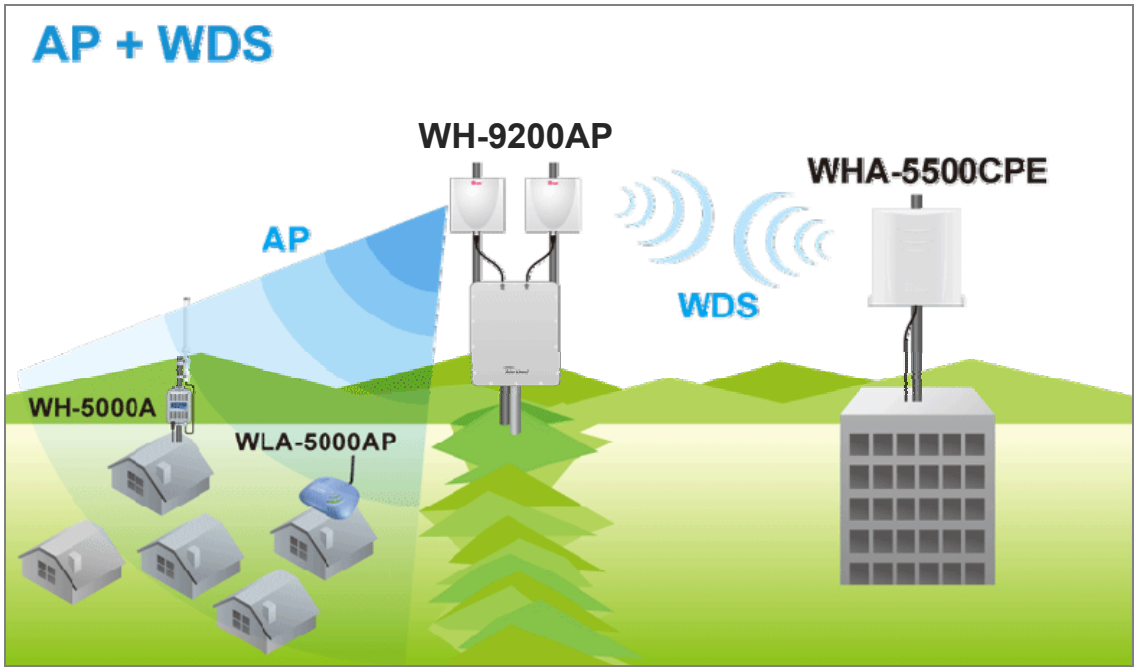


To configure the AP mode, please refer to Section 3.1 Access Point Mode……

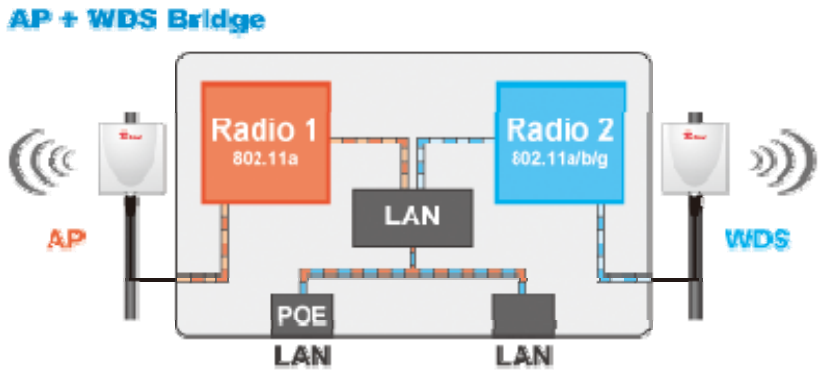
To configure the Client mode, please refer to Section 3.3 Client Mode ……

2.7 AP + WDS Bridge / WDS Bridge + AP Mode

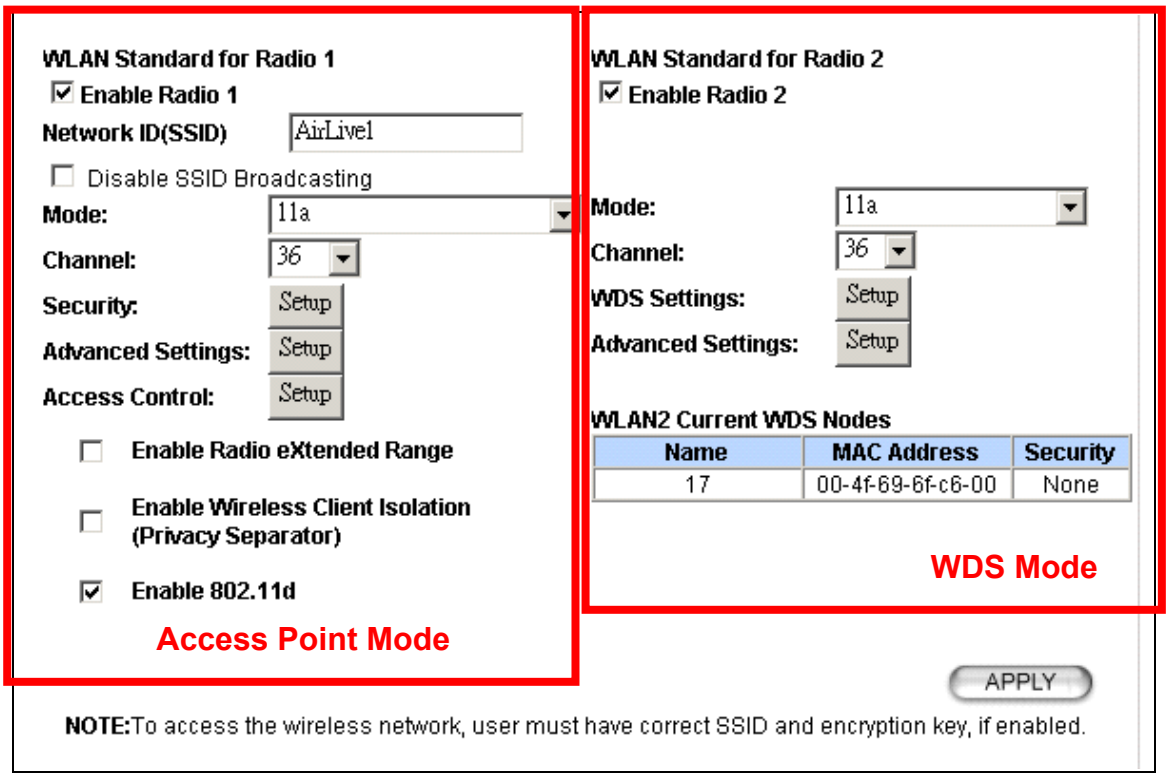
In this mode, one Radio is in Access Point mode and the other in WDS Bridge Mode.



- In this mode, the AP can act as a signal repeating station in a wireless backbone network. In addition, it can also function as directing station for NLOS application.
- The image in AP + WDS Bridge / WDS Bridge + AP mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.



The UI example of AP + WDS Bridge is as following:

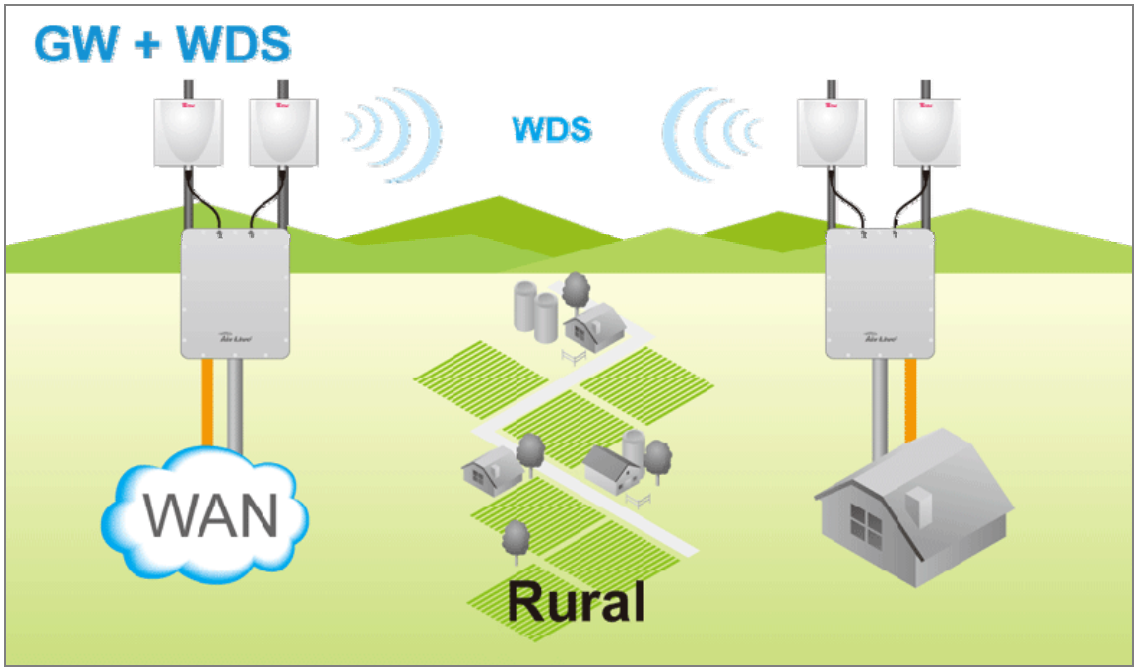


To configure the AP mode, Please refer to Section 3.1 Access Point Mode ……

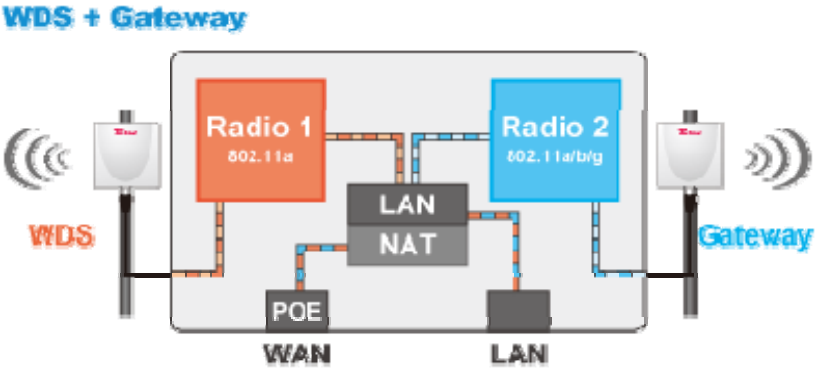
To configure the WDS mode, Please refer to Section 3.2 WDS Bridge Mode ……

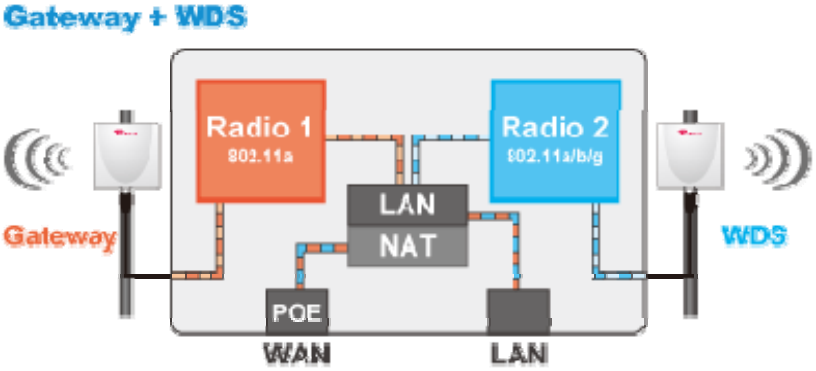
2.8 WDS + Gateway / Gateway + WDS Mode

In this mode, one radio acts as an AP router and the other a WDS bridge. One of the RJ-45 ports as the WAN interface to the internet.

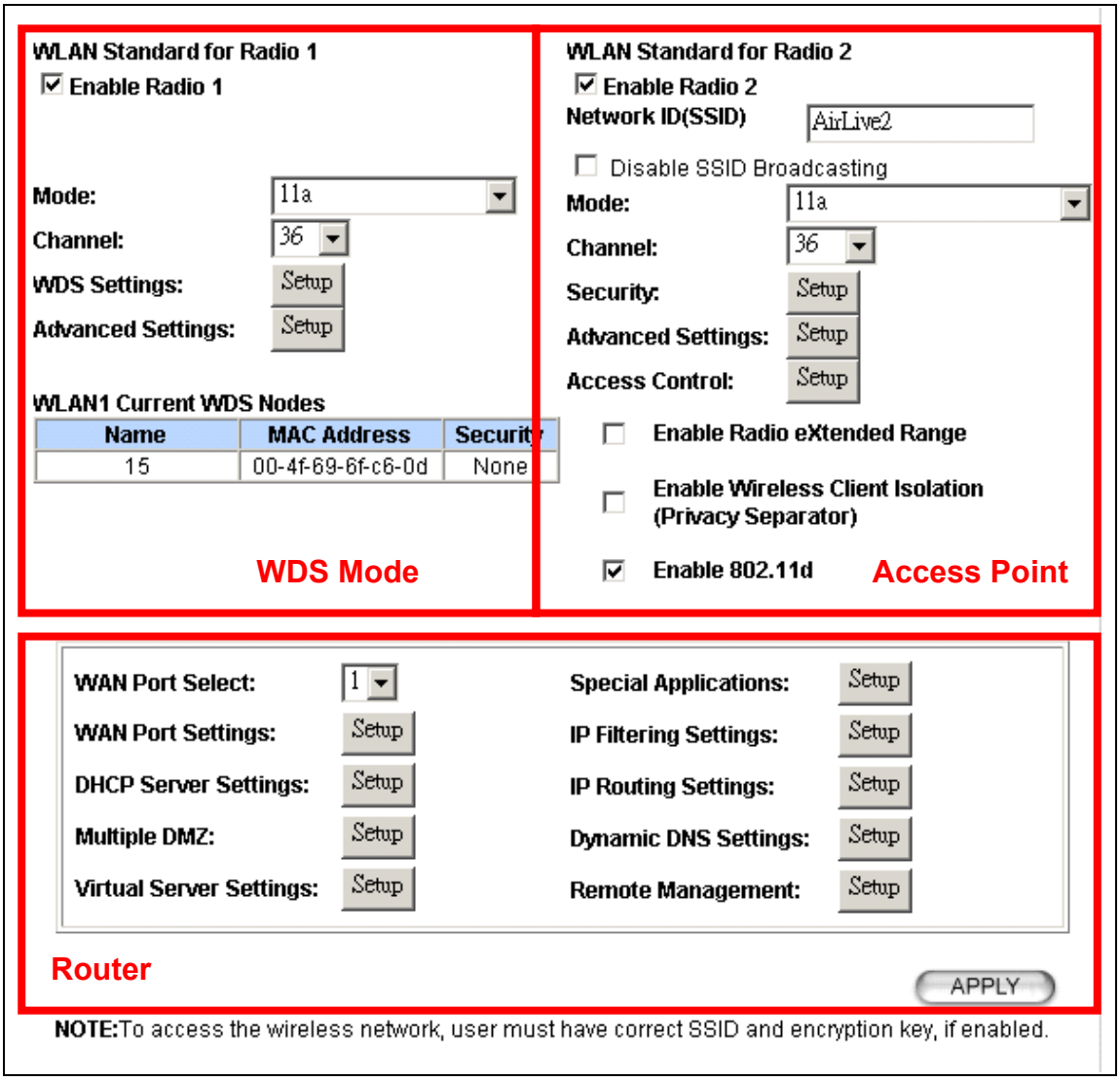


- The remote location can access the internet by way of this Access Point which acts as a gateway device of the network.
- The image in WDS + Gateway / Gateway + WDS mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.





The UI example of AP + WDS Bridge is as following:



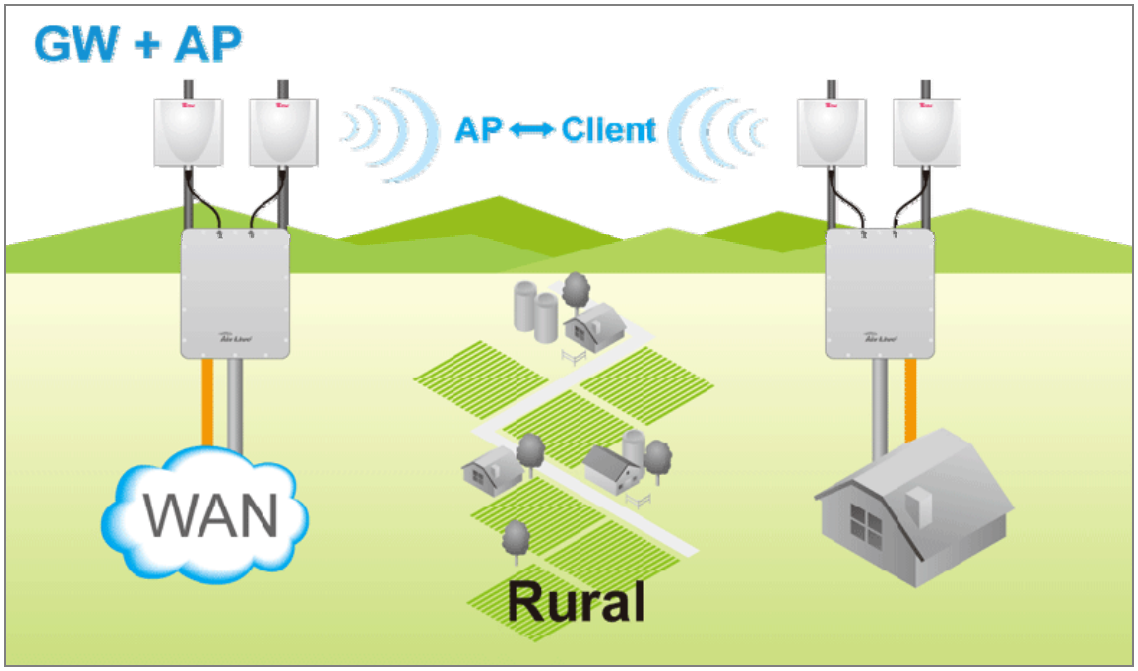
To configure the AP mode, Please refer to Section 3.1 Access Point Mode ……

To configure the WDS mode, Please refer to Section 3.2 WDS Bridge Mode ……

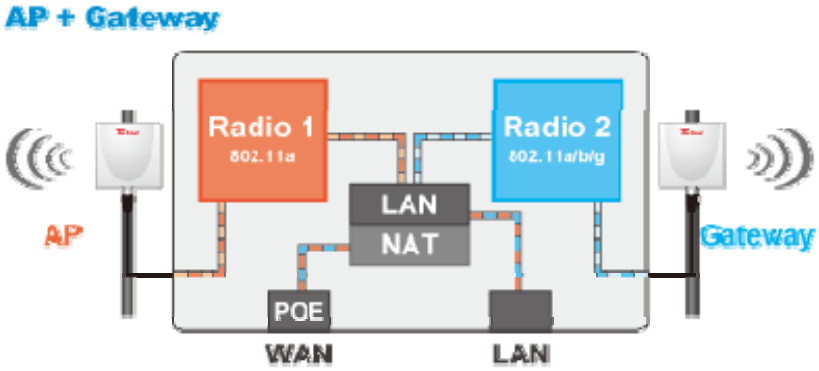
To configure the Gateway (Router) mode. Please refer to Section 3.4 Gateway Mode ……

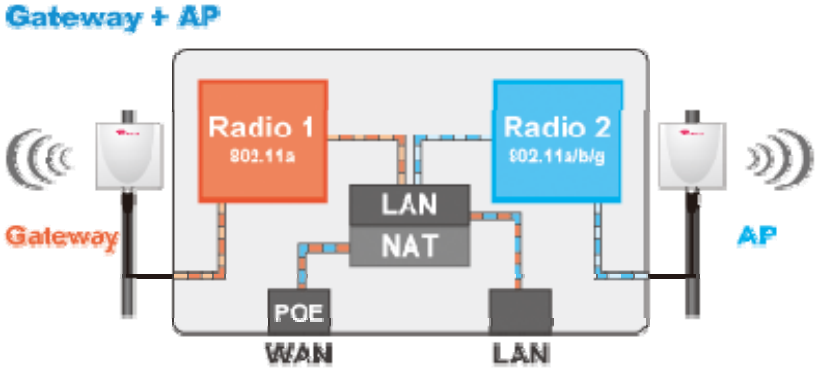
2.9 AP + Gateway / Gateway + AP Mode

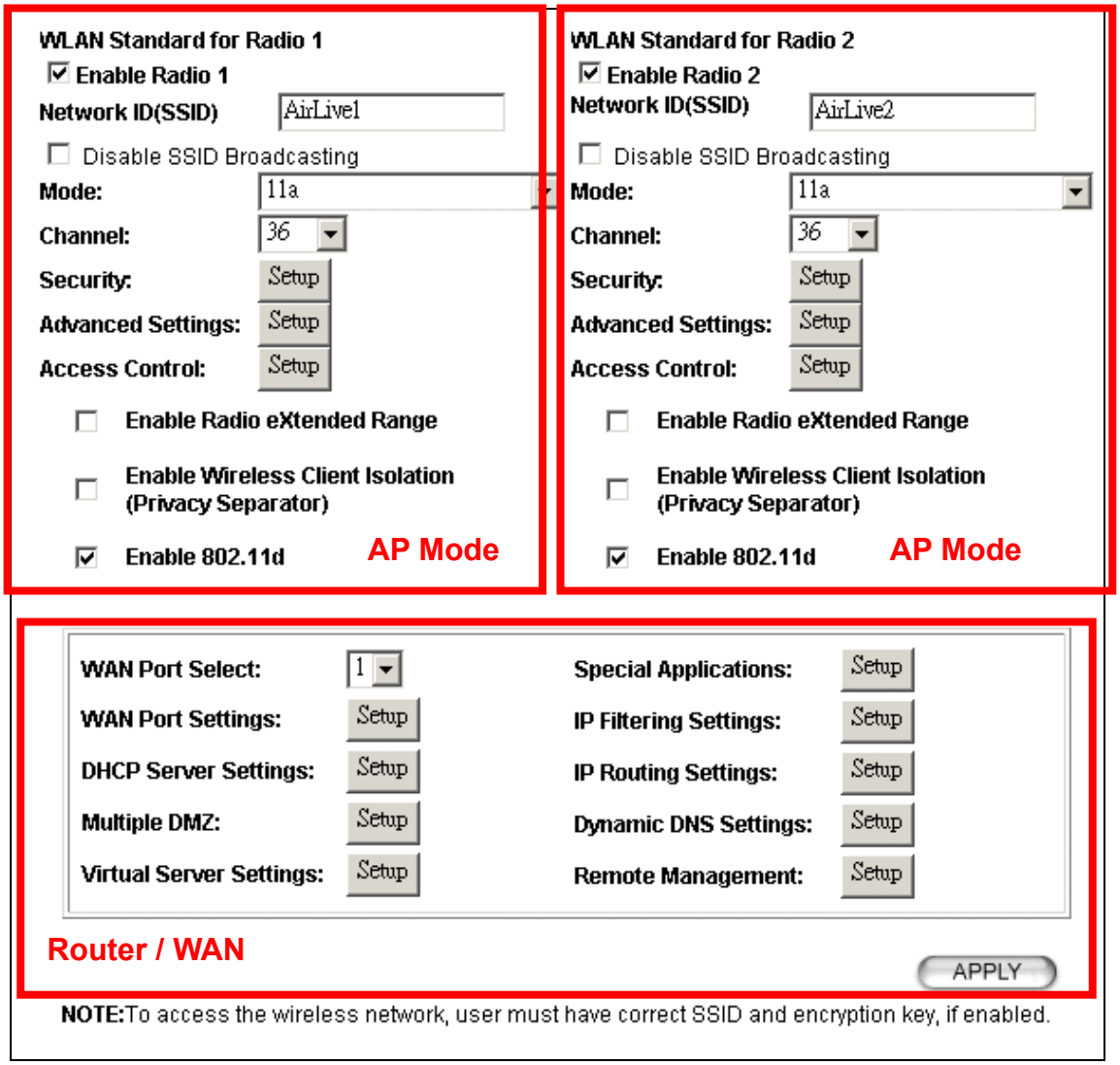
In this mode, one radio acts as an AP router and the other an Access Point. One of the RJ-45 ports as the WAN interface to the internet.



- The remote location can access the internet by way of this Access Point which acts as a gateway device of the network.
- The image in AP + Gateway / Gateway + AP mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.







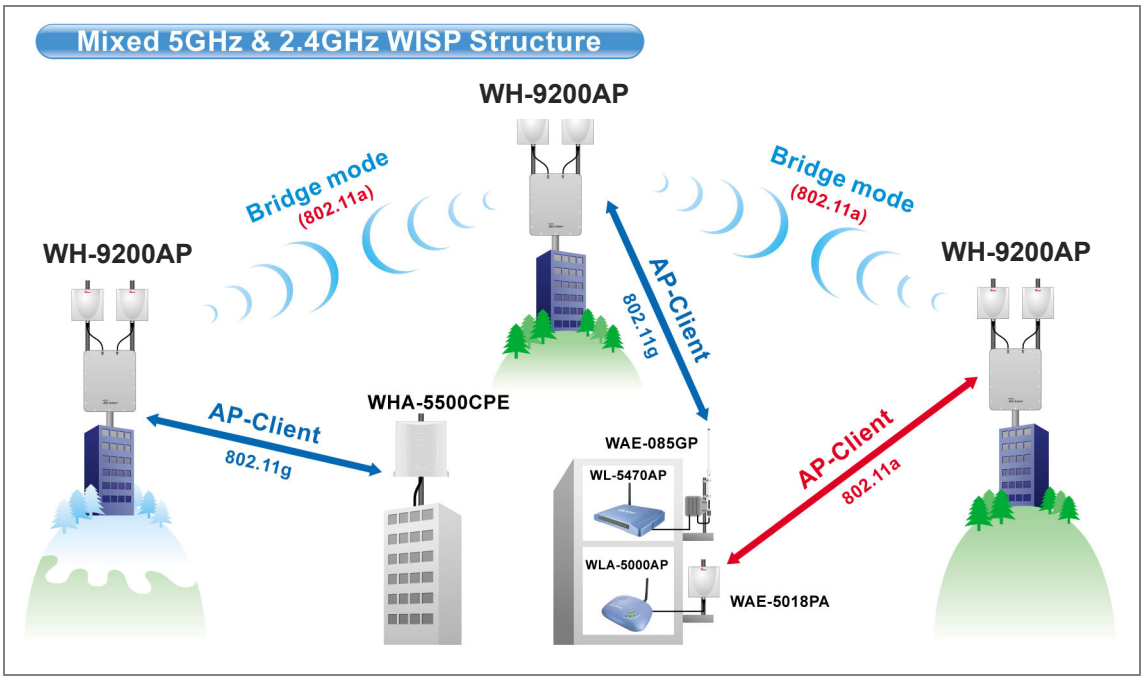
To configure the AP mode, Please refer to Section 3.1 Access Point Mode ……

To configure the WDS mode, Please refer to Section 3.2 WDS Bridge Mode ……

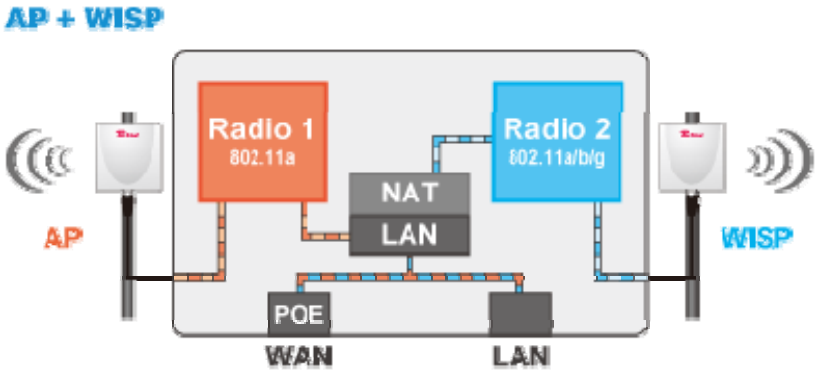
To configure the Gateway (Router) mode, Please refer to Section 3.4 Gateway Mode ……

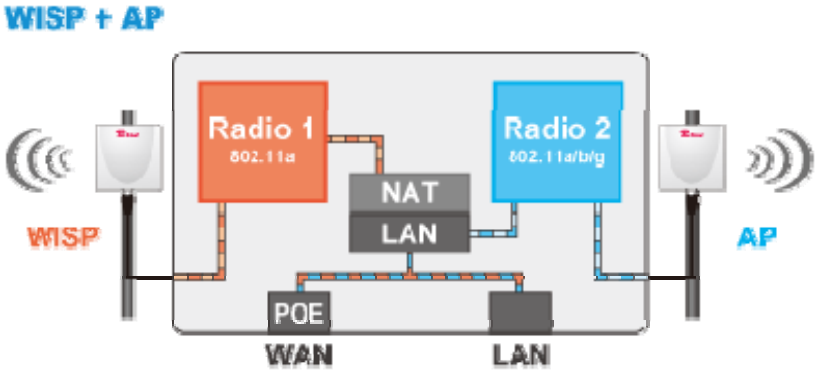
2.10 AP + WISP / WISP + AP Mode

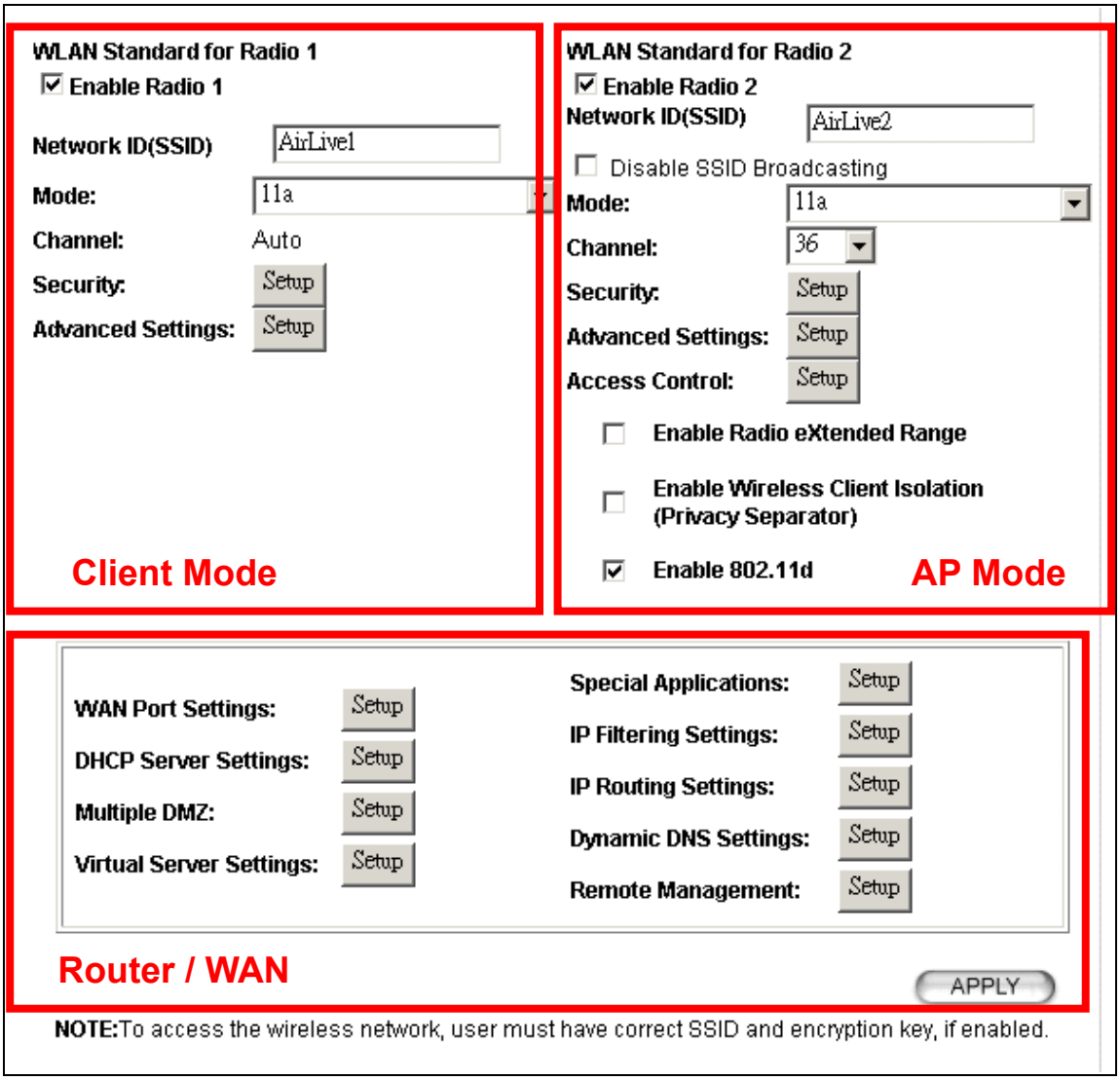
In this mode, one radio acts as an AP and the other acts as an client router. One of the RJ-45 ports as the WAN interface to the internet.



- The remote location can access the internet by way of this Access Point which acts as a gateway device of the network.
- The image in AP + Gateway / Gateway + AP mode UI helps to indicate data flow related to the Wireless and the Ethernet ports.







To configure the AP mode, Please refer to Section 3.1 Access Point Mode ……

To configure the Client mode, Please refer to Section 3.3 Client Mode ……

To configure the Gateway (Router) mode, Please refer to Section 3.4 Gateway Mode ……

3 Wireless Settings

This section guides you to configure the mode of the Radio interface. Note that the radio can select either 11a or 11b/g mode.

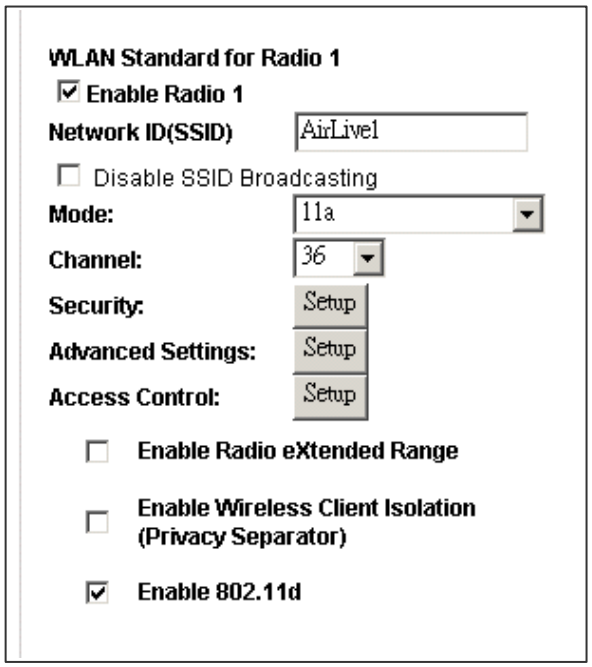
3.1 Access Point Mode

The Access Point mode is the most basic mode of multi-function Access Point. In this mode, the AP will act as a central hub for different Wireless LAN clients. Some hotspot Access Points requires 802.1x authenticator function to authenticate a user before providing internet service.



Access Point mode included in these operation modes: Dual AP, AP + Client, Client + AP, AP + WDS Bridge, WDS Bridge + AP, AP + Gateway, Gateway + AP, AP + WISP and WISP + AP modes.

Enable Radio: Use this check box to turn on or turn off the radio.



- **Network ID (SSID):** This is to change your SSID.
- **Disable SSID Broadcasting:** Enable the check box if you want to hide your SSID in the network. This prevent an un-welcomed client survey your radio.
- **Mode:** Connection modes on WH-9200AP and its wireless client. Note that the client must support the same

mode as WH-9200AP to connect.

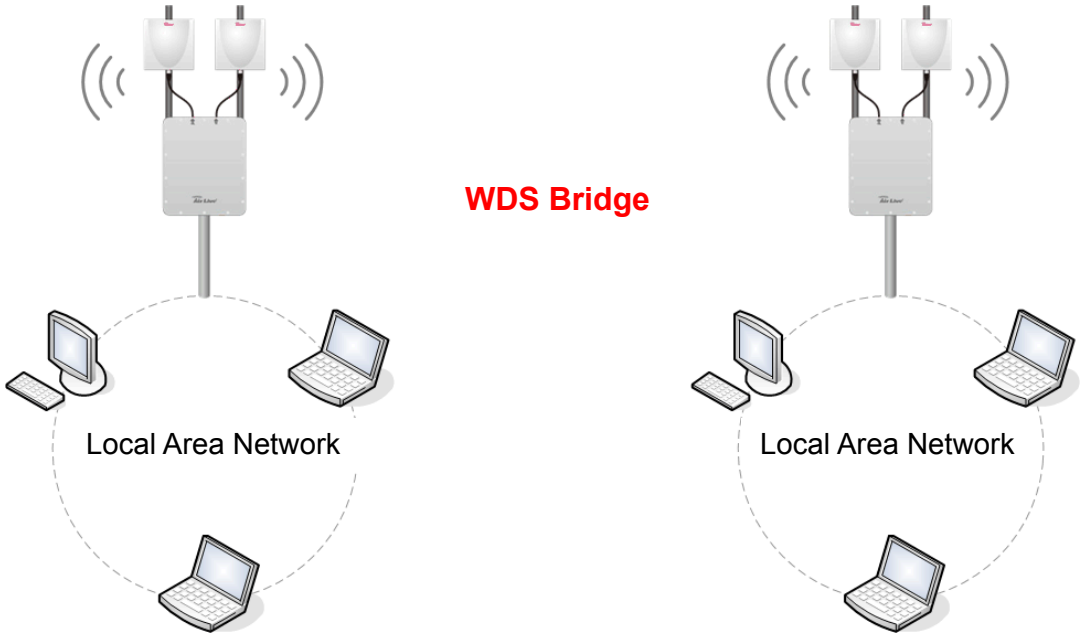
- **Channel:** 11a supports channel 36 to 64 and channel 100 to 140. 11g depends on the country, USA/Canada supports channel 1 to 11, Europe supports channel 1 to 13, Japan supports channel 1 to 13, France supports channel 10 to 13, and Span supports channel 10 to 11.
- **Enable Radio eXtended Range:** Check this box to extend the wireless coverage range, this is provided by Atheros's eXtended Range (XR) technology.
- **Enable Client Isolation (Privacy Separator):** This is to prohibit data transmission between each wireless client stations.
- **Enable 802.11d:** This is to prevent network loop applying to the spanning tree standard.

To configure the security connection, please refer to Section 3.6 Wireless Security Settings ……To configure the Advanced Settings, please refer to Section 3.7 Advanced Wireless Settings ……

To configure the access control, please refer to Section 3.8 Access Control Settings ……

3.2 WDS Bridge Mode

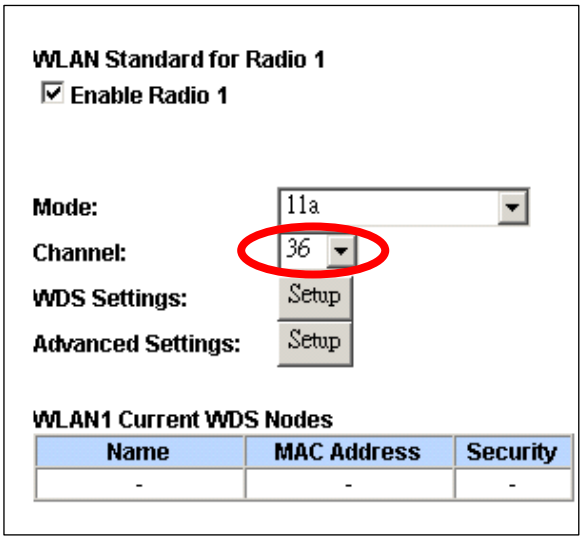
In this mode, 2 access points in two remote locations connect to each other to provide a wireless bridge between 2 remote LANs. It is mostly used by enterprise to connect 2 remote office's network together. The bridge modes are connected by using the WDS (Wireless Distribution System) technology.



WDS Bridge mode included in these operation modes: Duplex, Dual WDS Bridge, Separate Bridge, AP + WDS Bridge, and WDS Bridge + AP.

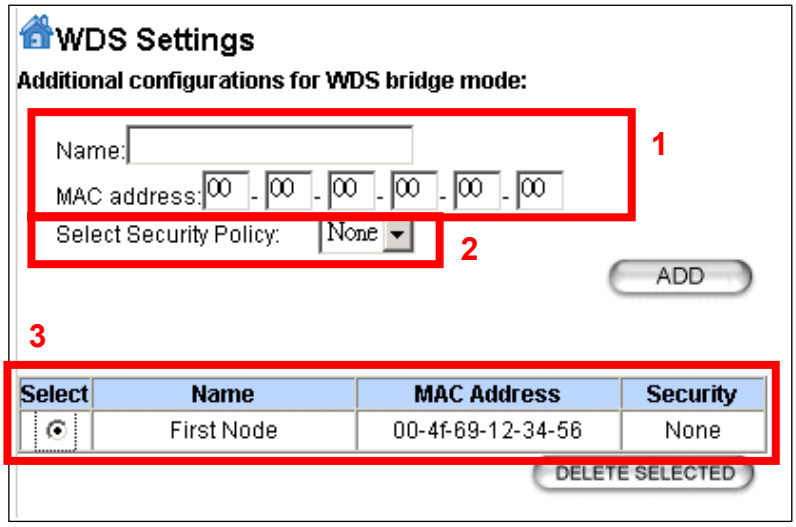
Under WDS mode, Access Points connects to each other with MAC ID address. It's important to register the device MAC ID between each other.

- **Enable Radio**: Use this check box to turn on or turn off the radio.
- **Mode:** Connection modes on WH-9200AP and its wireless client. Note that the client must support the same mode as WH-9200AP to connect.
- **Channel:** 11a supports channel 36 to 64 and channel 100 to 140. 11g depends on the country, USA/Canada supports channel 1 to 11, Europe supports channel 1 to 13, Japan supports channel 1 to 13, France supports channel 10 to 13, and Span supports channel 10 to 11.



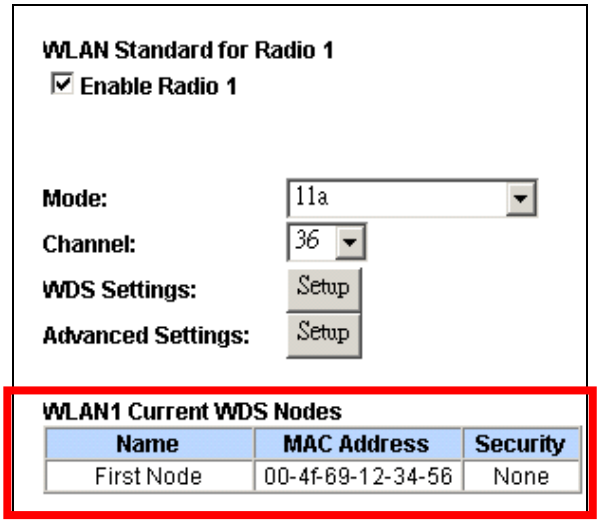
WDS Settings:

To configure WDS settings, click the WDS Settings **"Setup"** button, and the WDS Settings pop-up screen shows, please input the details of MAC ID address and desired name for remote device.



1. Enter the Name and MAC address of remote node which bridge to your WH-9200AP.
2. Only WEP security allowed in WDS mode, note that the remote node must use same security configuration as your WH-9200AP to communicate.
3. Click **"ADD"** button, the configured information of remote node shows.

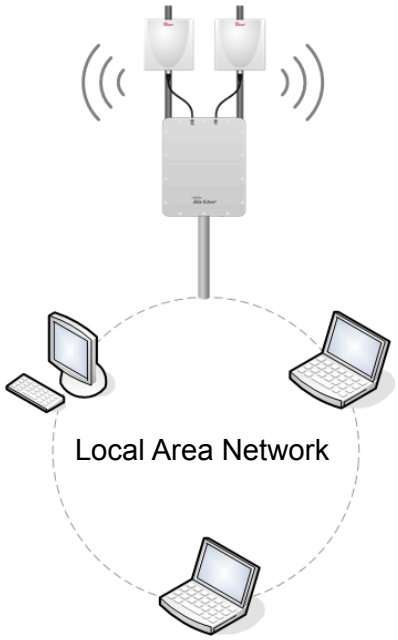
And the information shows in main configuration page as below:



To configure the Advanced Settings, please refer to Section 3.7 Advanced Wireless Settings ……

3.3 Client Mode

Also known as Ethernet Client. In this mode, the AP will act as a WLAN card to connect with the remote AP. Users can connect PC or local LAN to the Ethernet port of local LAN to the Ethernet port of the client mode AP. This mode is mostly used as a CPE device for WISP subscriber.

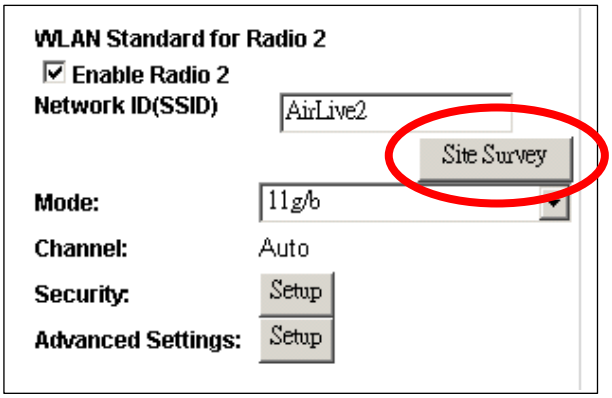


Client Mode

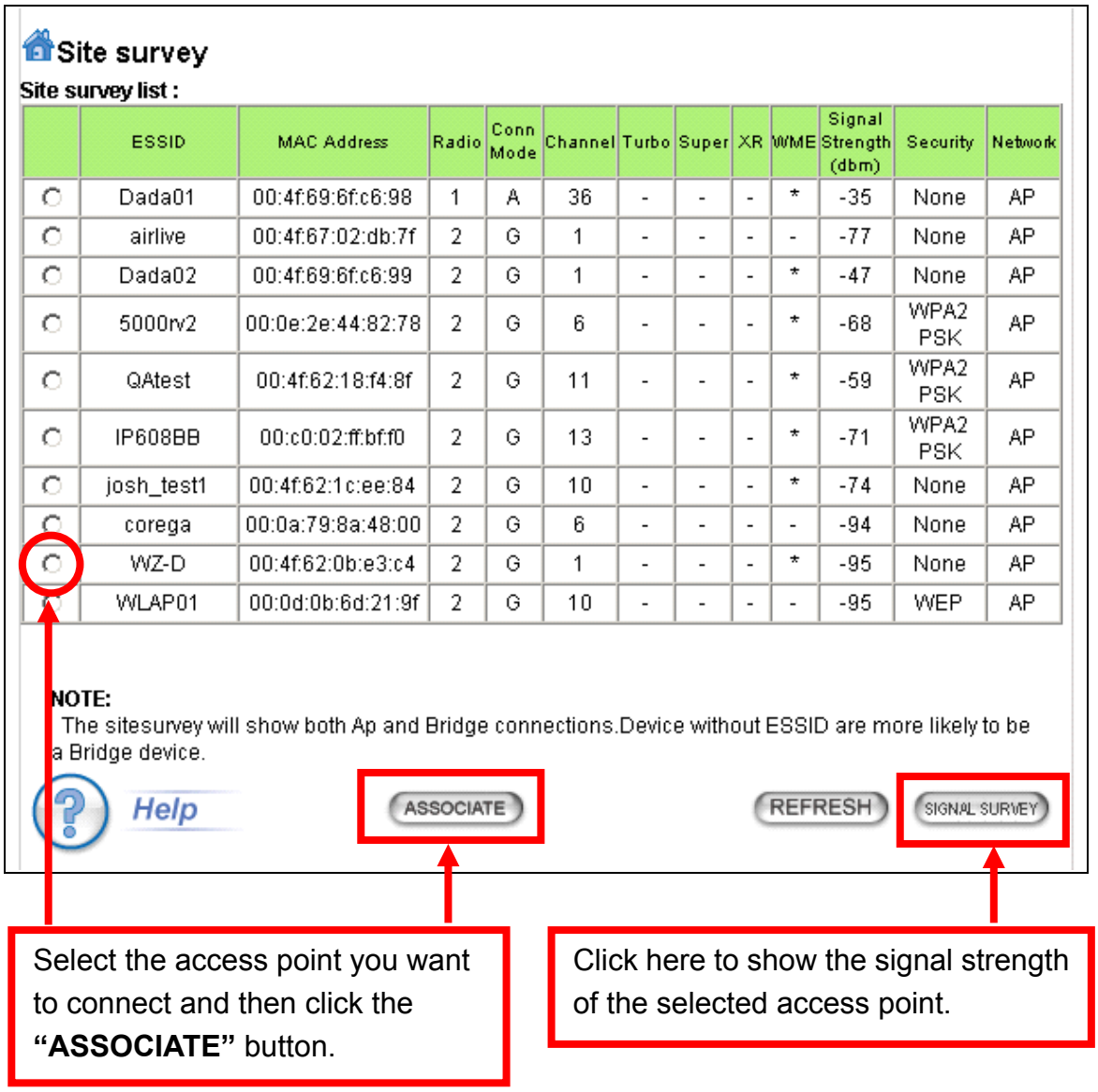


Client mode included in these operation modes: AP + Client, Client + AP, AP + WISP, and WISP + AP.

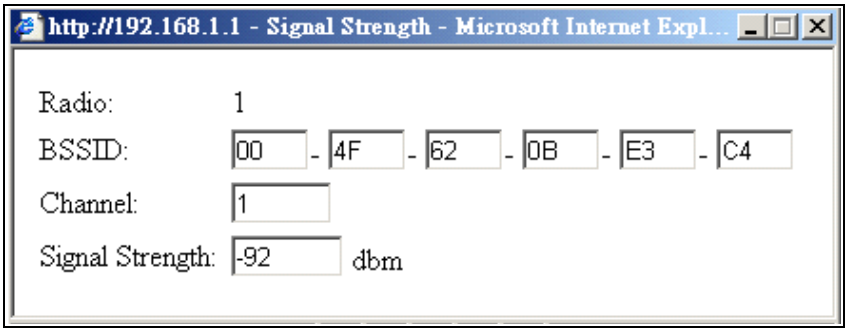
1. To connect to an access point, use the **"Site Survey"** button to find the Access Point.



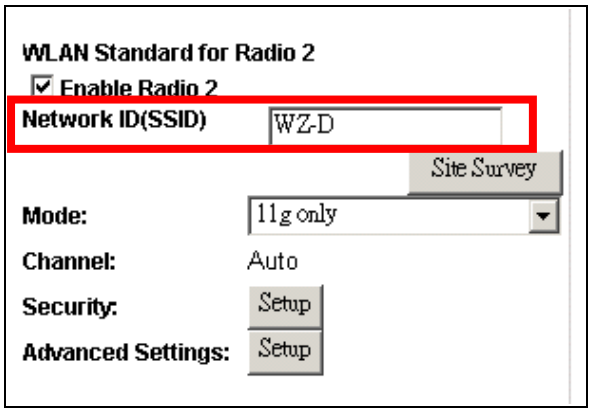
2. The Site Survey pop up window then shows up and lists available access point with relative information.



3. The Signal Survey pop up windows shows as following:



4. After the access point is selected, its SSID shows automatically in the Network ID (SSID) field.

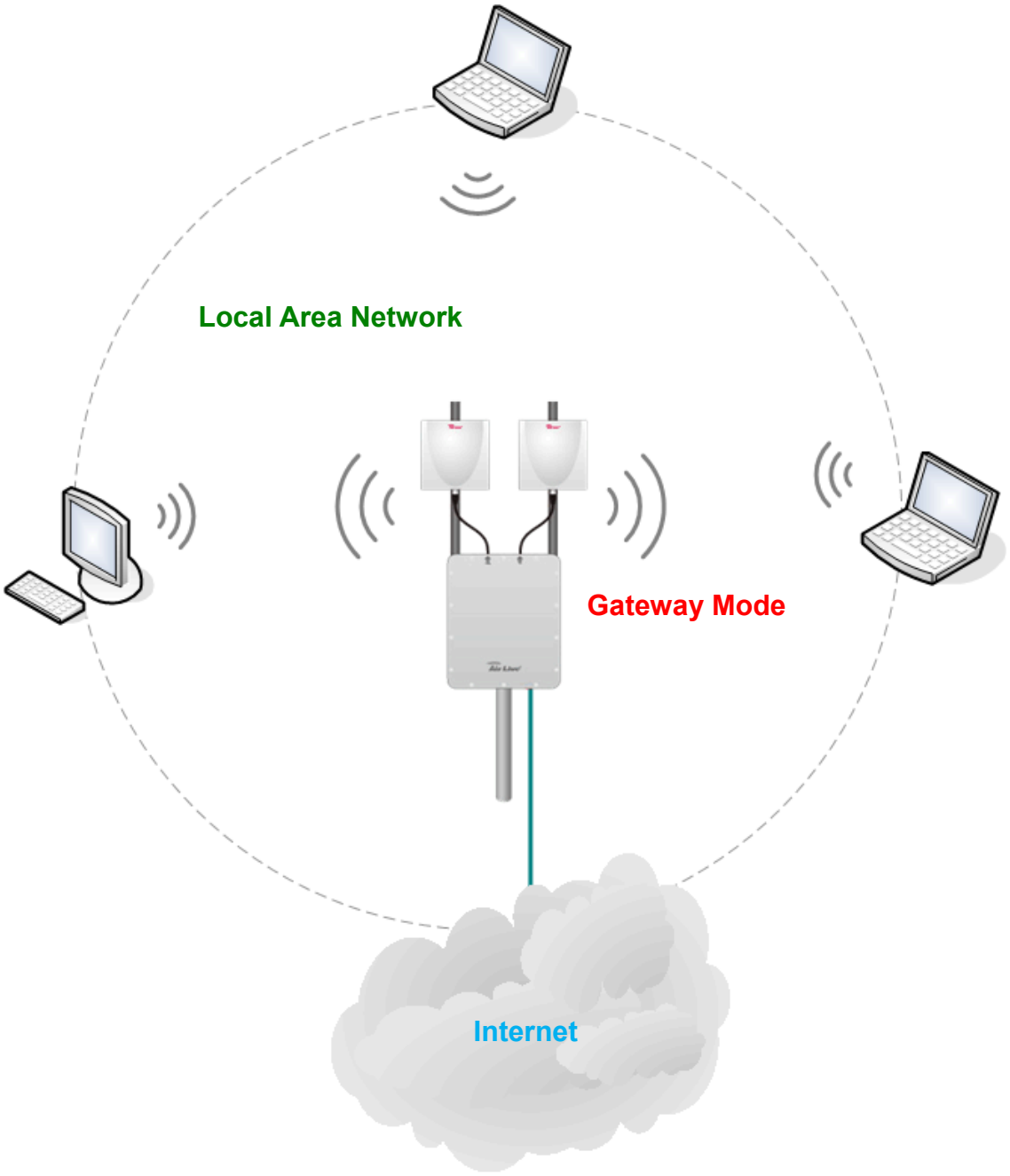


To configure the Security, please refer to Section 3.6 ……

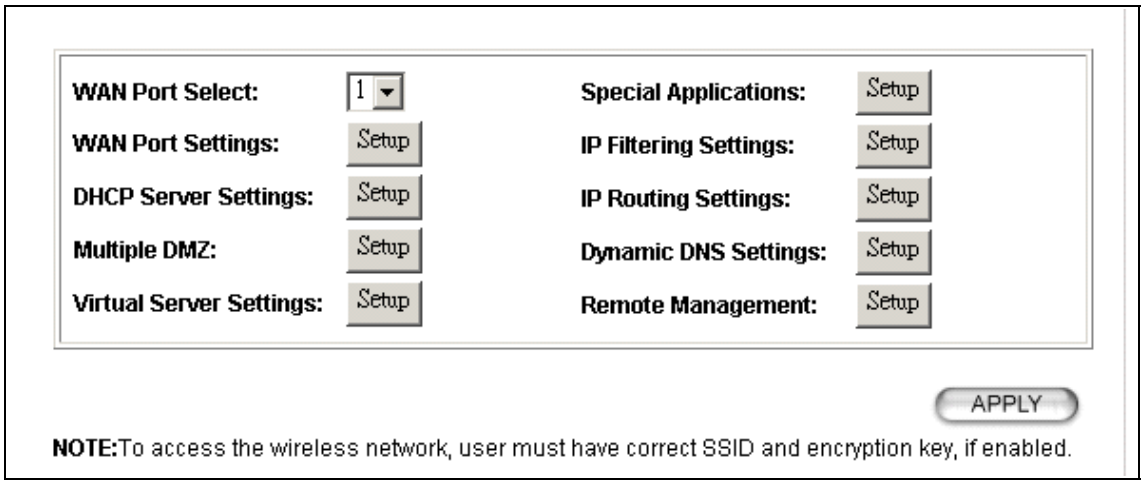
To configure the Advanced Settings, please refer to Section 3.8……

3.4 Gateway (AP Router) Mode

In Gateway mode, router functions are added between one Ethernet port and other network interfaces. Therefore, the ISP subscriber can share the ISP connection without need for extra router.



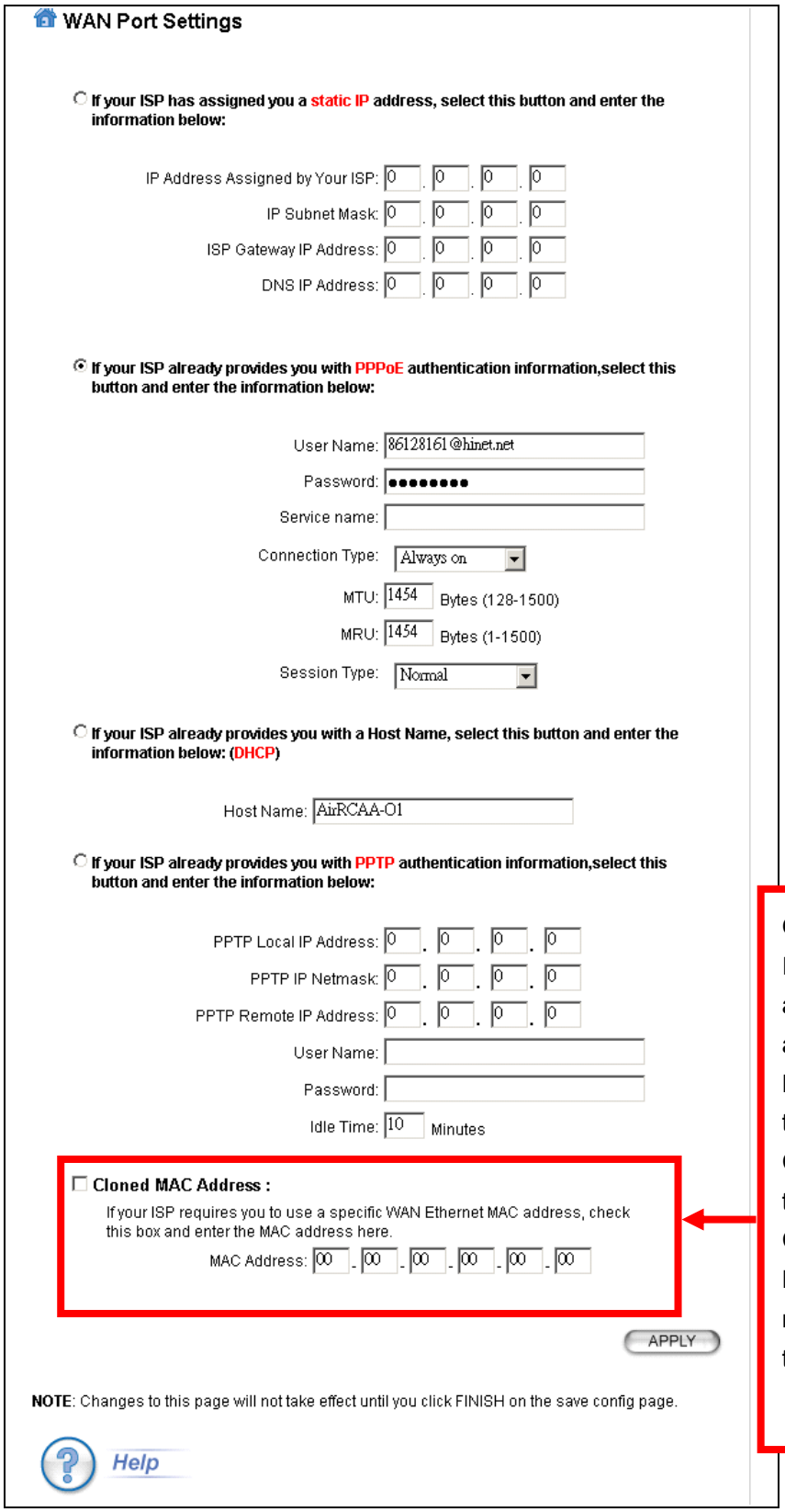
Gateway mode acts both in AP and Router which included in these operation modes: AP + Gateway and Gateway + AP.



WAN Port Select: Either the Ethernet port 1 or port 2 can be set to be the WAN port.

3.4.1 WAN Port Settings

- Click the Setup button to configure the WAN interface.
- WH-9200AP provides 4 methods for client to access the internet. This depends on the location and the service which the ISP provides. You need to contact the ISP for detail information.

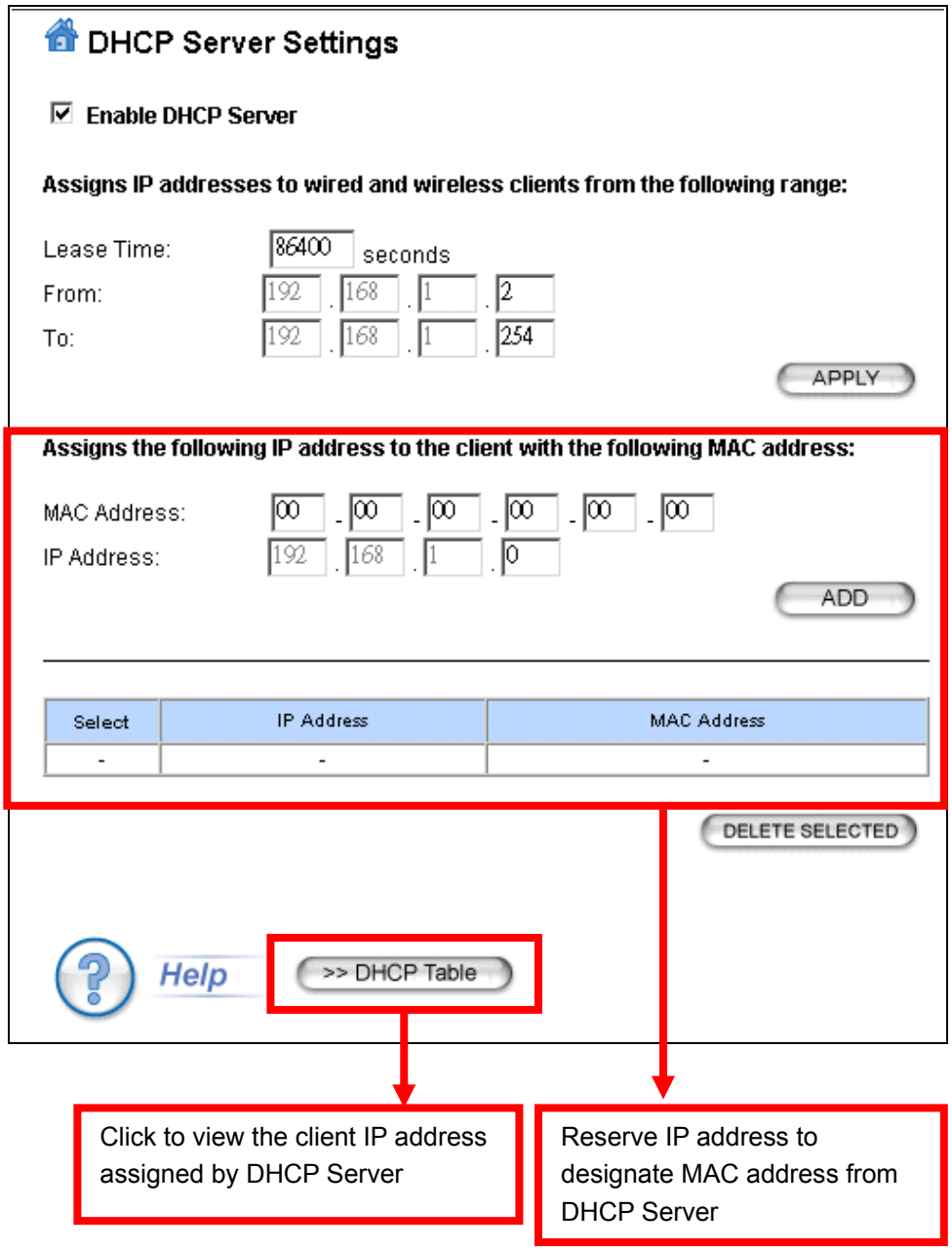


Clone MAC address: If your ISP allows only one MAC address for its internet access and you need more than one PC/Laptop/Server to access the internet, you can use the Clone MAC address to solve this issue.
Copy either MAC of the PC/Laptop/Server which needs to access the internet in the MAC address fields.

3.4.2 DHCP Server Settings

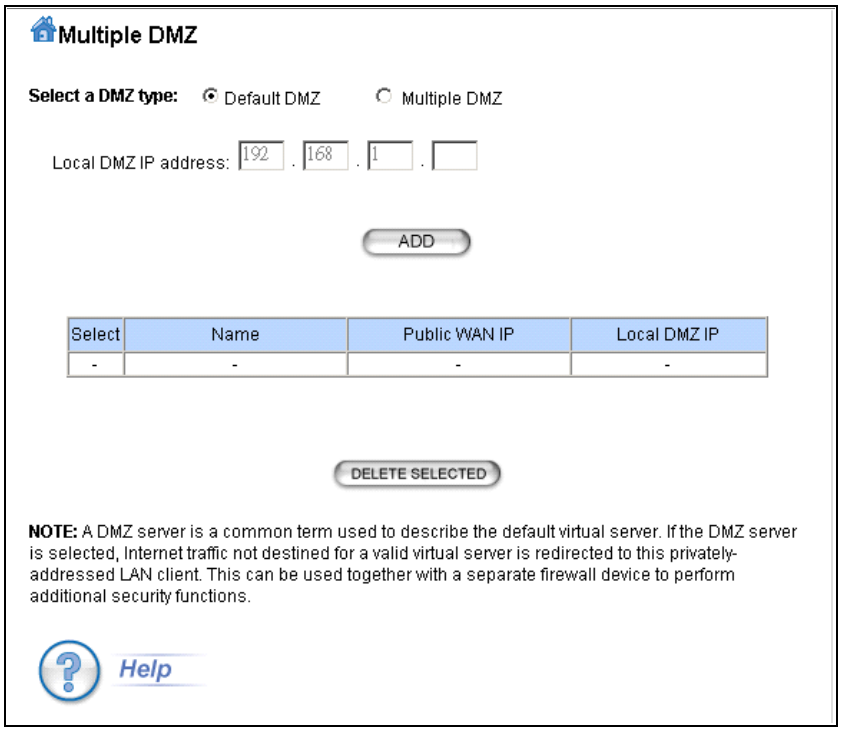
DHCP Server Settings is to assign private IP address to the devices in your local area network (LAN). Note that WH-9200AP keeps the IP address of 192.168.1.1 and act as the default gateway of the LAN.

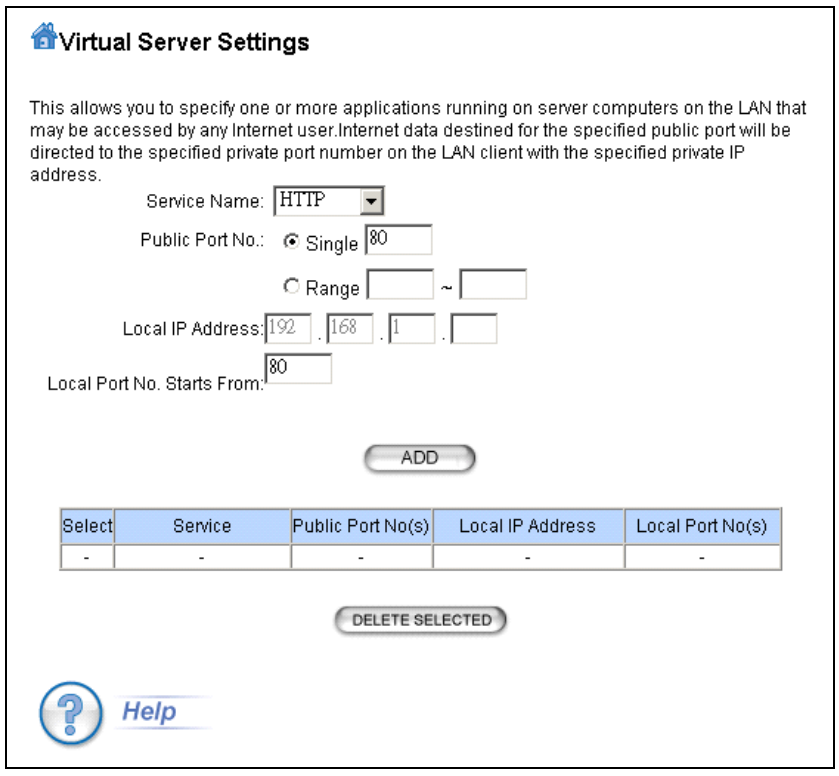
You can assign IP address to MAC address; the DHCP server will keep the IP for the MAC address.



3.4.3 DMZ & Virtual Server

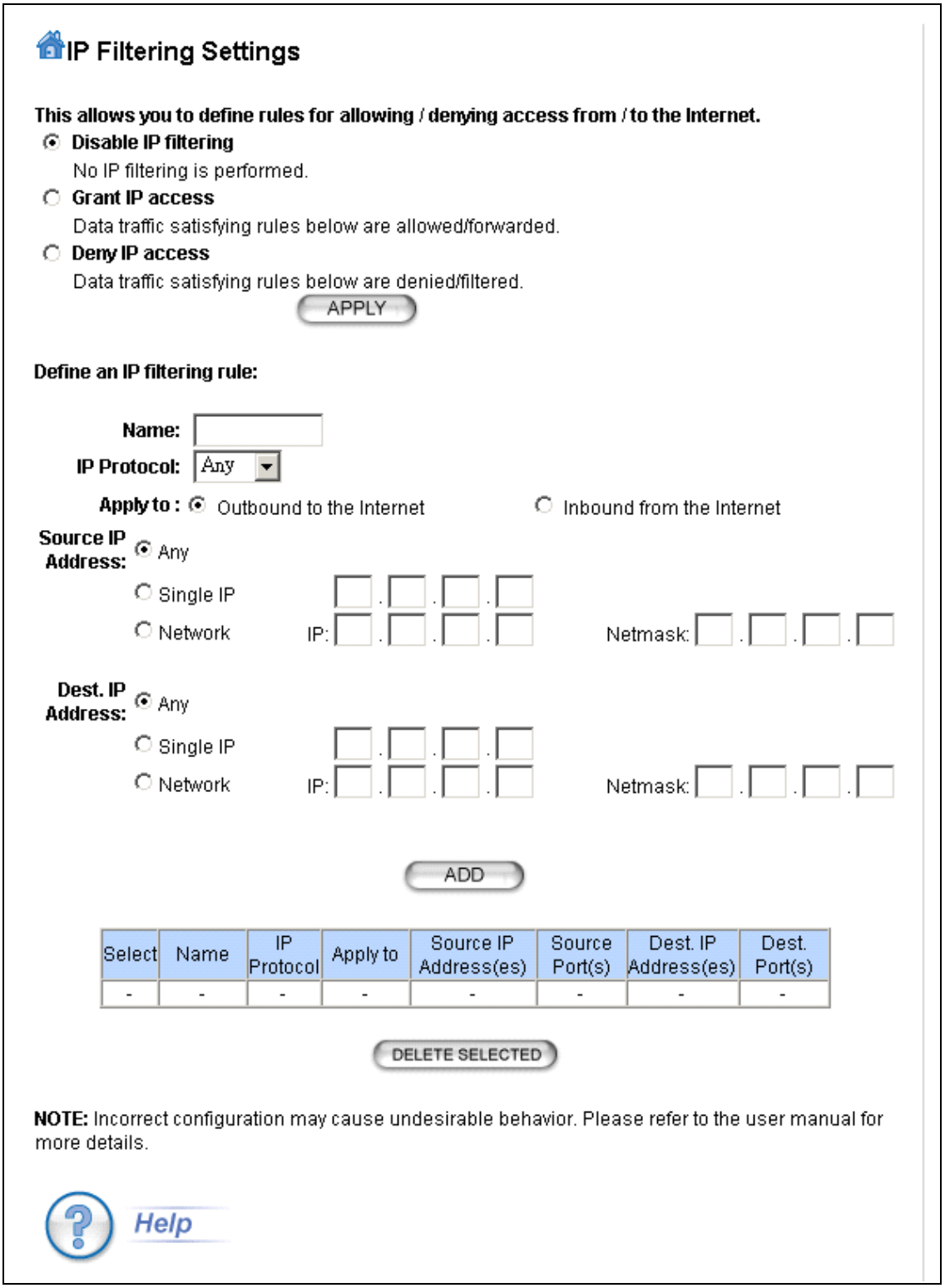
You can use DMZ and Virtual Server Settings to provide connection on internet. For example, you can have your own web server at home and provide access on internet. This will need port 80 by default for Virtual Server Settings.





3.4.4 IP Filter Settings

IP filtering is simply a mechanism that decides which types of IP datagrams will be processed normally and which will be discarded.



This allows you to define rules for allowing / denying access from / to the Internet.

Please do set both inbound/outbound in order to get complete connection. Only inbound or outbound will not allow to get response from the destination IP.

Disable IP filtering: No IP filtering is performed.

Grant IP access: Data traffic satisfying rules below are allowed/forwarded.

Deny IP access: Data traffic satisfying rules below are denied/filtered.

You can also define IP filtering rule, such as:

Name; IP Protocol; Apply to either Outbound to the Internet or Inbound from the Internet; Source IP Address and Dest. (Destination) IP Address.

To grant or deny IP address, select **ADD** or **Delete Selected**.

3.4.5 IP Routing Settings

The IP Routing Settings allows you to configure routing feature in the gateway, the settings is normally no need to change in gateway mode.

IP Routing Settings

Dynamic Routing

Select the routing protocol scheme used for the router's LAN / WAN port.

- (•) **Disable**
- ( ) **RIP**

APPLY

Static Routing

This allows you to manually configure static network routes. Static routes will override routes learned by standard routing protocol discover methods.

Destination IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

(•) Gateway IP Address: 0 . 0 . 0 . 0

( ) Interface: wan

Metric Count: 1

ADD

To add a static route, enter the information above and click **ADD**.

IP Routing Table

Select	Destination IP Address	Subnet Mask	Gateway IP Address<	Interface	Flag	Metric
-	192.168.1.0	255.255.255.0	-	lan	U	0
-	239.0.0.0	255.0.0.0	-	lan	U	0

DELETE SELECTED

To delete a static route from the table, select the route and click **DELETE SELECTED**.

NOTE: Changes to the routing table will take effect immediately.

Help

Dynamic Routing:

Select the routing protocol scheme used for the router's LAN / WAN port.

Static Routing:

This allows you to manually configure static network routes. Static routes will override routes learned by standard routing protocol discover methods.

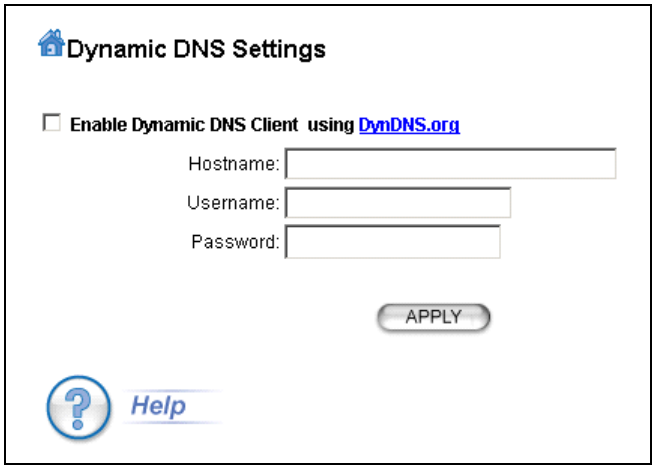
IP Routing Table:

To delete a static route from the table, select the route and click DELETE SELECTED.

Note: Changes to the routing table will take effect immediately.

3.4.6 Dynamic DNS (DDNS) Settings

Dynamic DNS (DDNS) allows you to create a hostname that points to your dynamic IP or static IP address or URL. WH-9200AP provide Dynamic DNS client using DynDNS, please visit http://www.dyndns.org for detail.

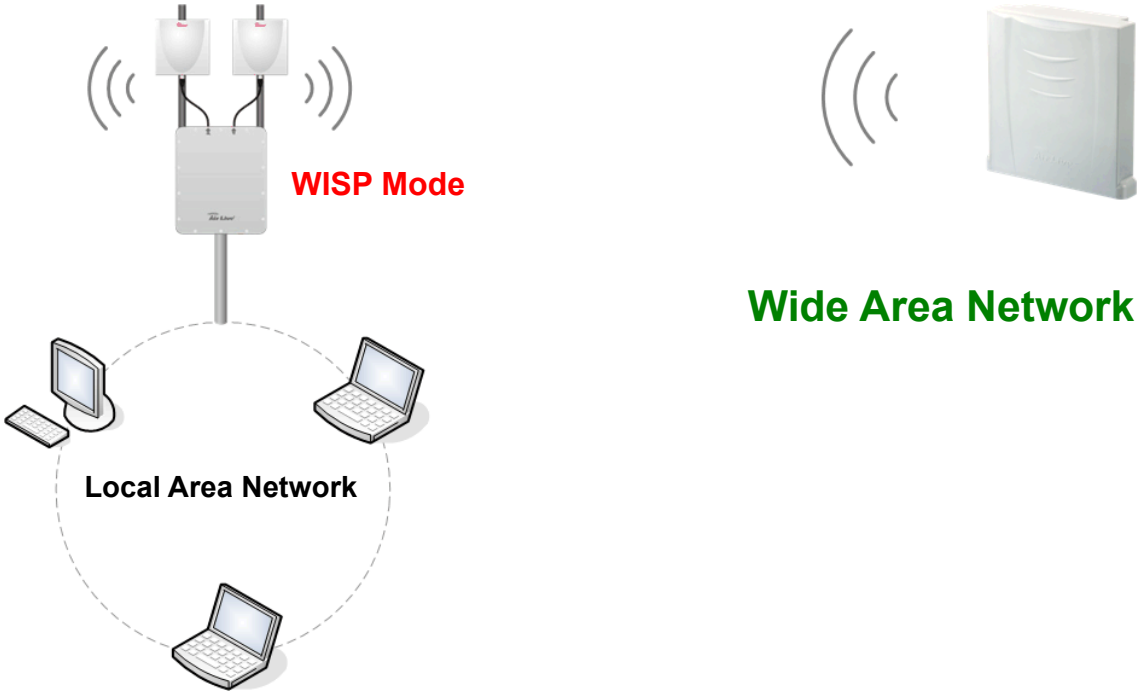


The Remote Management setting allows you to enable web server access from internet, note that this needs to configure a virtual server for your WH-9200AP. You can enable to the **"Response to WAN Ping"** to allow remotely ping your WH-9200AP.



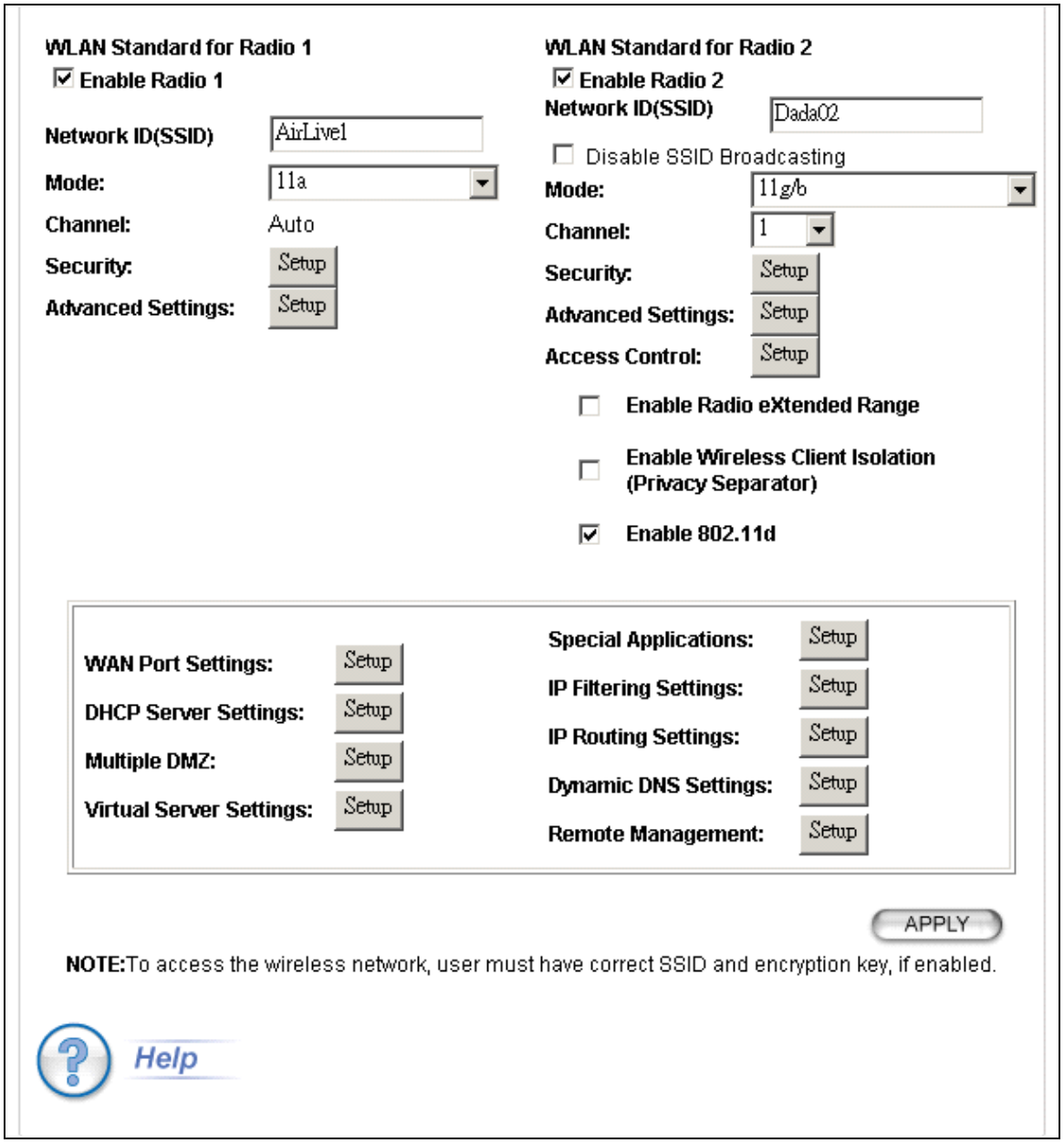
3.5 WISP Mode

In WISP mode, the AP will behave just the same as the Client mode for wireless function. However, router functions are added between the wireless WAN side and the Ethernet LAN side. Therefore, the WISP subscriber can share the WISP connection without need for extra router.



WISP mode acts both in AP and Router which included in these operation modes: AP + WISP and WISP + AP.

In WISP + AP mode, the Radio 1 is actually a wireless client of the WISP wireless node and also the gateway of the local area network.



Please refer to **Section 3.4** for gateway settings.

To configure the AP mode, Please refer to Section 3.1 Access Point Mode ……

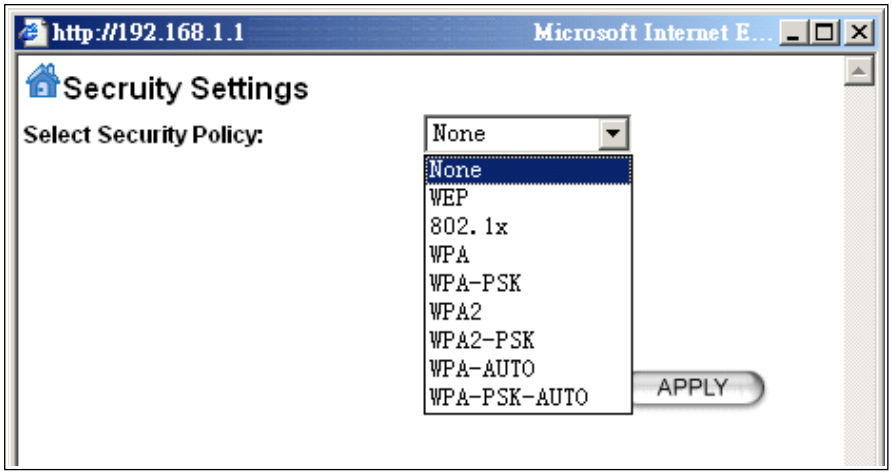
To configure the WDS mode, Please refer to Section 3.3 Client Mode ……

To configure the Gateway (Router) mode, Please refer to Section 3.4 Gateway Mode ……

3.6 Wireless Security

The wireless security is to configure a secure connection between two wireless devices.

WH-9200AP provides WEP, 802.1x, WPA, WPA-PSK, WPA2, WPA2-PSK, WPA-AUTO and WPA-PSK-AUTO security policy.



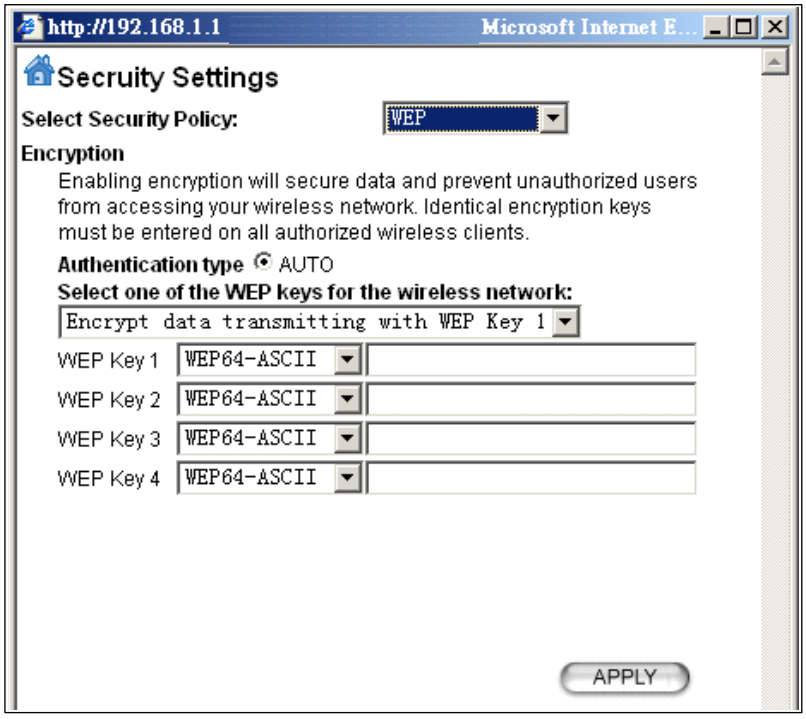
WEP

WEP allows you to use data encryption to secure your data from being eavesdropped by malicious people. It allows 3 types of key: 64 (WEP64), 128 (WEP128), and 152 (WEP152) bits. You can configure up to 4 keys using either ASCII or Hexadecimal format.

Key Settings: The length of a WEP64 key must be equal to 5 bytes, a WEP128 key is 13 bytes, and a WEP152 key is 16 bytes.

Key Index: You have to specify which of the four keys will be active.

Once you enable the WEP function, please make sure that both the WH-9200AP and the wireless client stations use the same key.

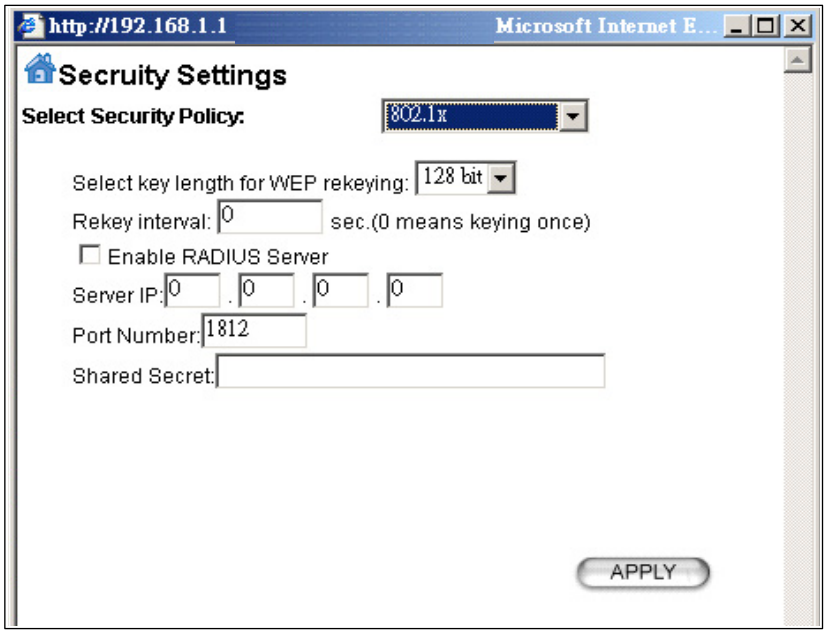


Some wireless client cards only allow Hexadecimal digits for WEP keys.
Please note that when configuring WEP keys, a WEP128 ASCII key looks like "**This is a key**"(13 characters), while a WEP128 Hex key looks like "**546869732069732061206b6579**"(26 HEX) (hexadecimal notation are 0-9 and A-F).

802.1X

802.1x allows users to leverage a RADIUS server to do association authentications. You can also enable dynamic WEP key (128 bit) to have data encryption. Here you do not have to enter the WEP key manually because it will be generated automatically and dynamically.

Rekey interval is time period that the system will change the key periodically. The shorter the interval is, the better the security is.



Server IP and Shared Secret: If you have connect AP to a RADIUS server behind, key in the Server IP and share secret, it will redirect incoming connection request first to this RADIUS for Authentication. In general you don't have to change Port Number, which is 1812 by default and used by most RADIUS server.

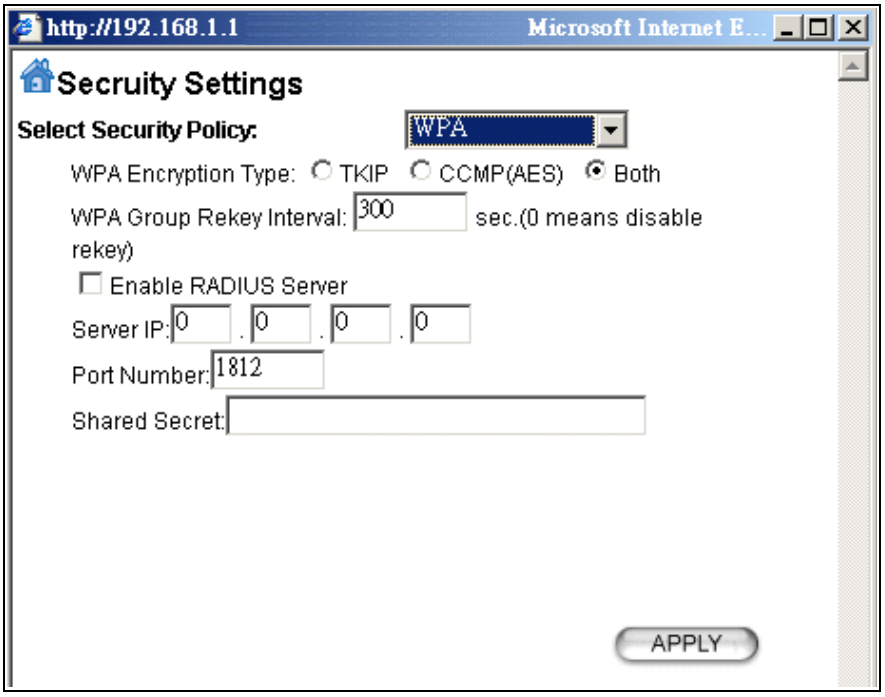


After you have finished the configuration wizard, you have to configure the RADIUS Settings in Advanced Settings in order to make the 802.1x function work.

Share secret is the key for AP to communicate with RADIUS server, check with your Authentication provider for more details.

WPA

Wi-Fi Protected Access (WPA) requires a RADIUS server available in order to do authentication (same as 802.1x), thus there is no shared key required.

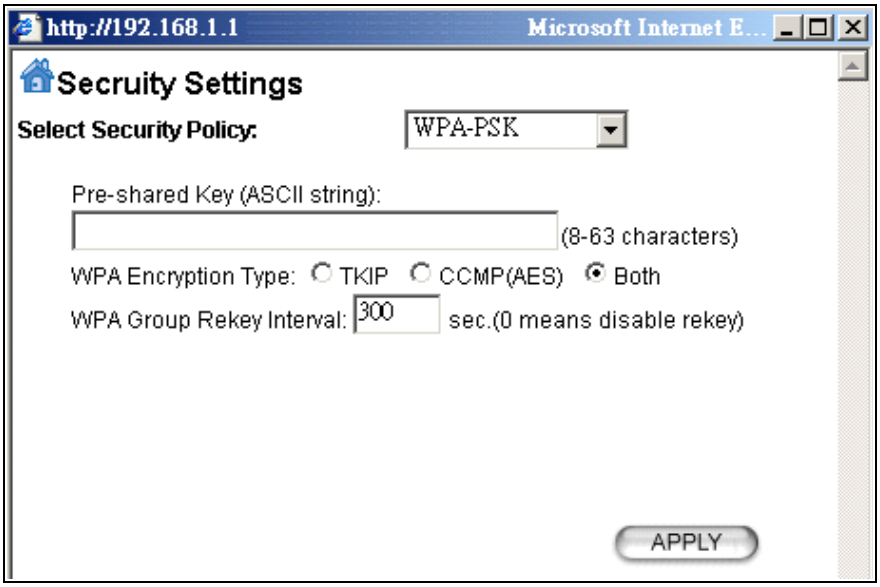


Encryption Type: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.

Group Rekey Interval: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

WPA-PSK

Wi-Fi Protected Access (WPA) with Pre-Shared Key (PSK) provides better security than WEP keys. It does not require a RADIUS server in order to provide association authentication, but you do have to enter a shared key for the authentication purpose. The encryption key is generated automatically and dynamically.



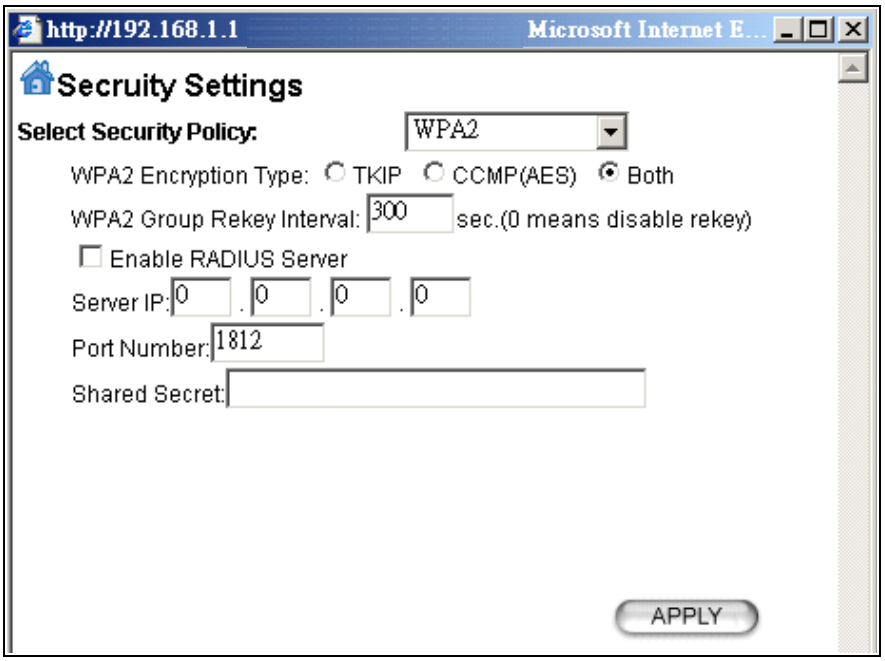
Pre-shared Key: This is an ASCII string with 8 to 63 characters. Please make sure that both the WH-9200AP and the wireless client stations use the same key.

Encryption Type: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.

Group Rekey Interval: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

WPA2

WPA2 stands for Wi-Fi Protected Access 2. It provides stronger data protection and network access control then WPA. Only authorized users can access the wireless networks.

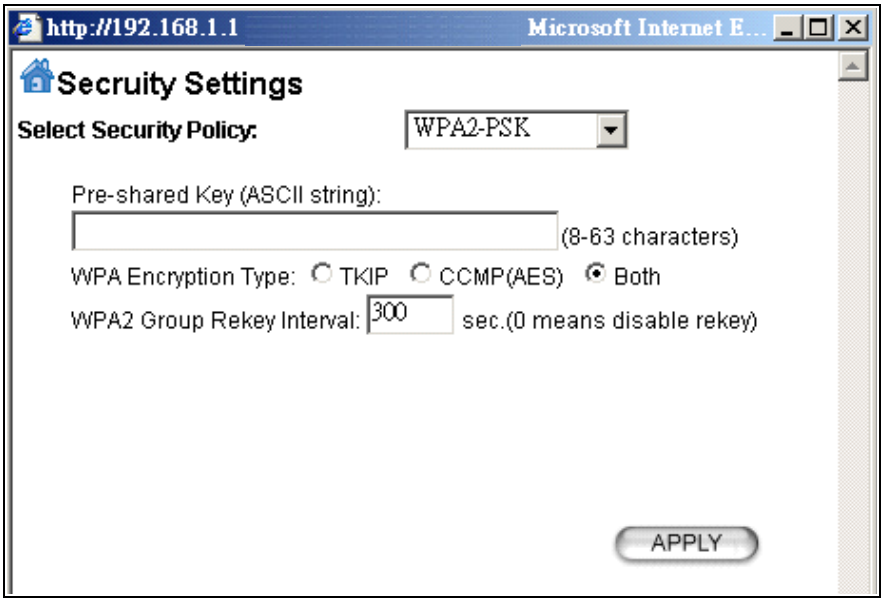


Encryption Type: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.

Group Rekey Interval: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

WPA2-PSK

Enter the Pre-shared Key to initiate WPA2 security. All devices try to access the network should have the matching encryption key.

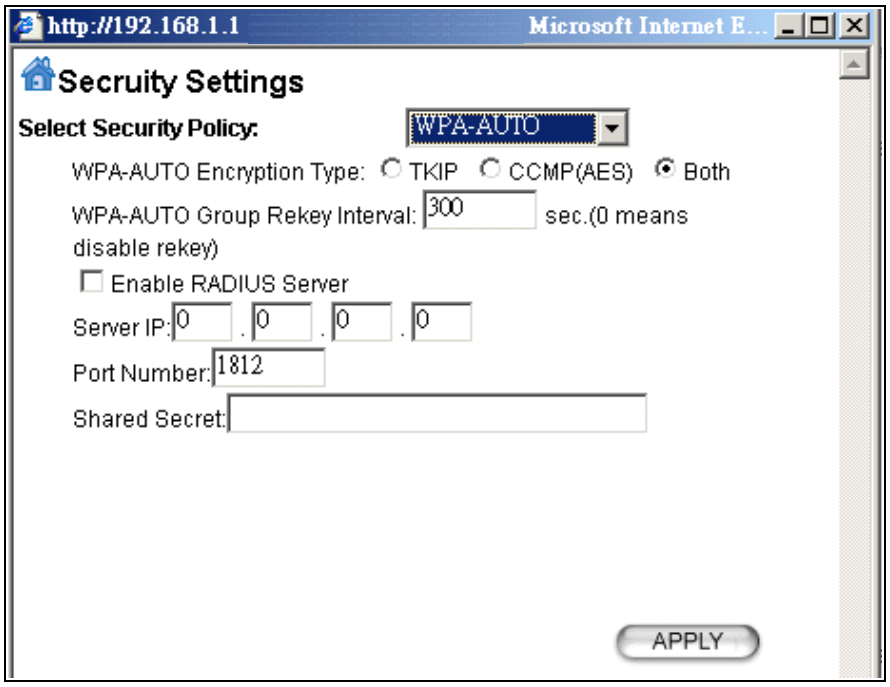


Pre-shared Key: This is an ASCII string with 8 to 63 characters. Please make sure that both the WH-9200AP and the wireless client stations use the same key.

Encryption Type: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.

Group Rekey Interval: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

WPA-AUTO

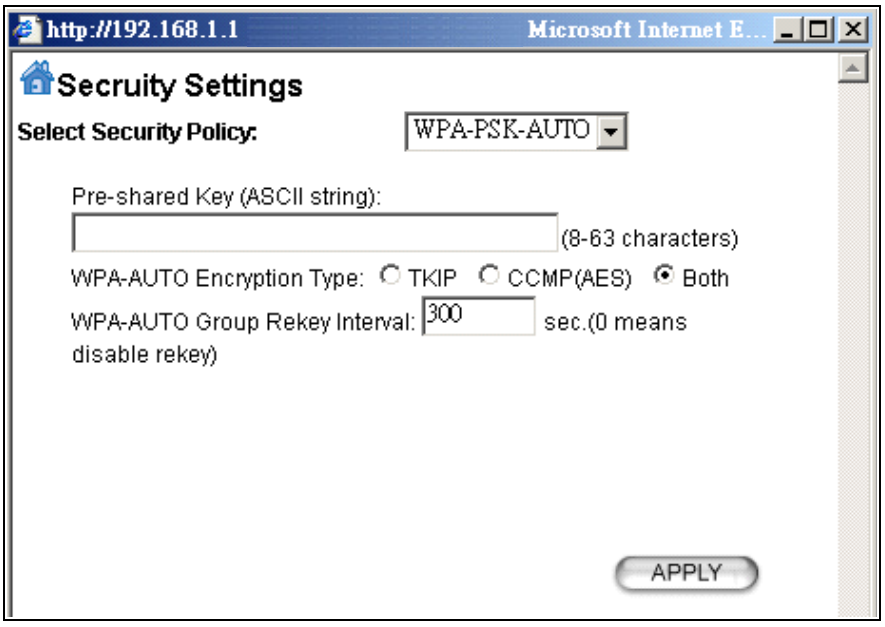


Encryption Type: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.

Group Rekey Interval: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

WPA-PSK-AUTO

WPA-PSK-AUTO tries to authenticate wireless clients using WPA-PSK or WPA2-PSK.



Pre-shared Key: This is an ASCII string with 8 to 63 characters. Please make sure that both the WH-9200AP and the wireless client stations use the same key.

Encryption Type: There are two encryption types **TKIP** and **CCMP (AES)**. While CCMP provides better security than TKIP, some wireless client stations may not be equipped with the hardware to support it. You can select **Both** to allow TKIP clients and CCMP clients to connect to the Access Point at the same time.

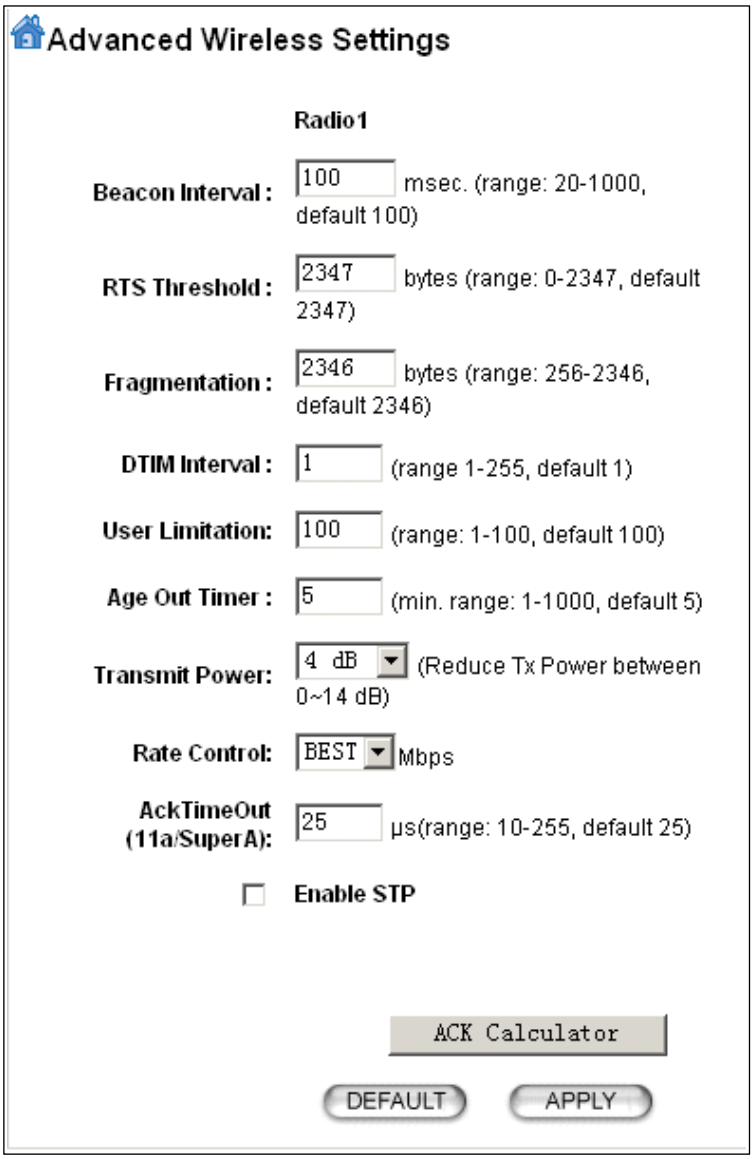
Group Rekey Interval: A group key is used for multicast/broadcast data, and the re-key interval is time period that the system will change the group key periodically. The shorter the interval is, the better the security is. The default is 300 sec.

3.7 Advanced Wireless Settings

When click on Advanced Setup button under client mode, a pop-up window appears and show parameter as follow:

Beacon Interval: The WH-9200AP broadcasts beacon frames regularly to announce its existence. The beacon Interval specifies how often beacon frames are transmitted in time unit of milliseconds.

RTS Threshold: RTS/CTS frames are used to gain control of the medium for transmission. Any unicast (data or control) frames larger than specified RTS threshold must be transmitted following the RTS/CTS handshake exchange mechanism. The RTS threshold should have a value between 256-2347 bytes, with a default of 2347. It is recommended that this value does not deviate from the default too much.



Fragmentation: When the size of a unicast frame exceeds the fragmentation threshold, it will be fragmented before the transmission. It should have a value of 256-2346 bytes, with a default of 2346. If you experience a high packet error rate, you should slightly decrease the Fragmentation Threshold.

DTIM Interval: The WH-9200AP buffers packets for stations that operate in the power-saving mode. The Delivery Traffic Indication Message (DTIM) informs such power-conserving stations that there are packets waiting to be received by them. The DTIM interval specifies how often the beacon frame should contain DTIMs.

User Limitation: The range of user limitation is from 1 to 100.

Age Out Timer: Set the age out time. The default is 300 sec.

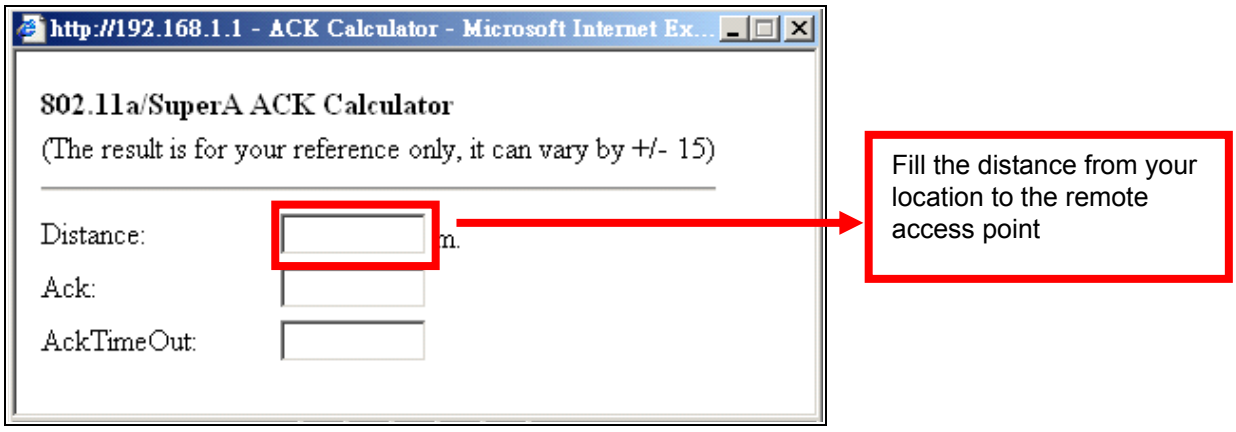
Transmit Power: Transmit power output depends upon the size and RF characteristics because that will determine the number of APs, channels, and need for antennas.

Rate Control: Limit the wireless data rate to the selected number.

Enable STP: Spanning Tree Protocol prevents the condition known as a bridge loop.

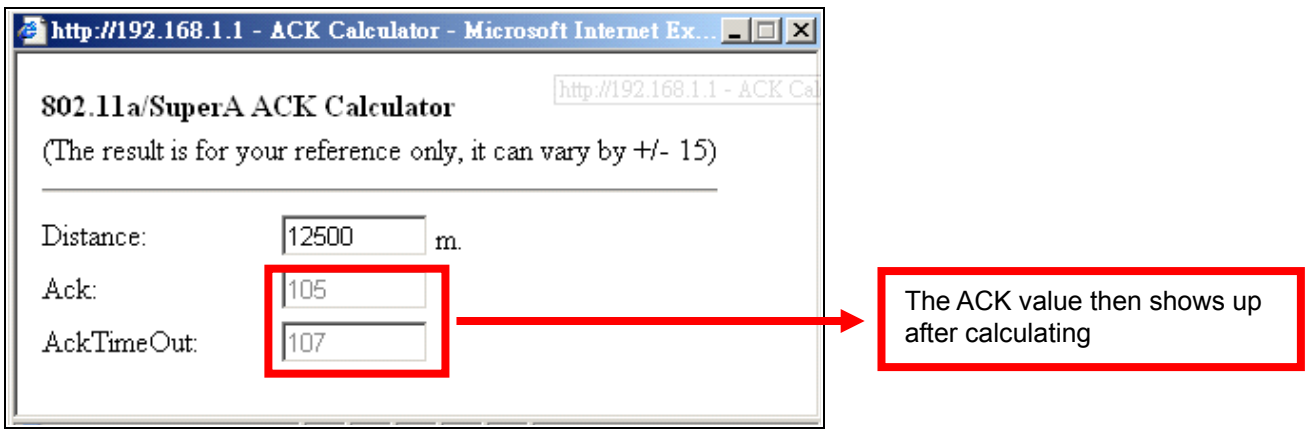
Ack TimeOut: The **"ACK time-out"** determines how long the program waits after receiving a packet from a file stream to determine that stream to be a complete file.

The following windows pops up when click on “ACK Calculator” button:

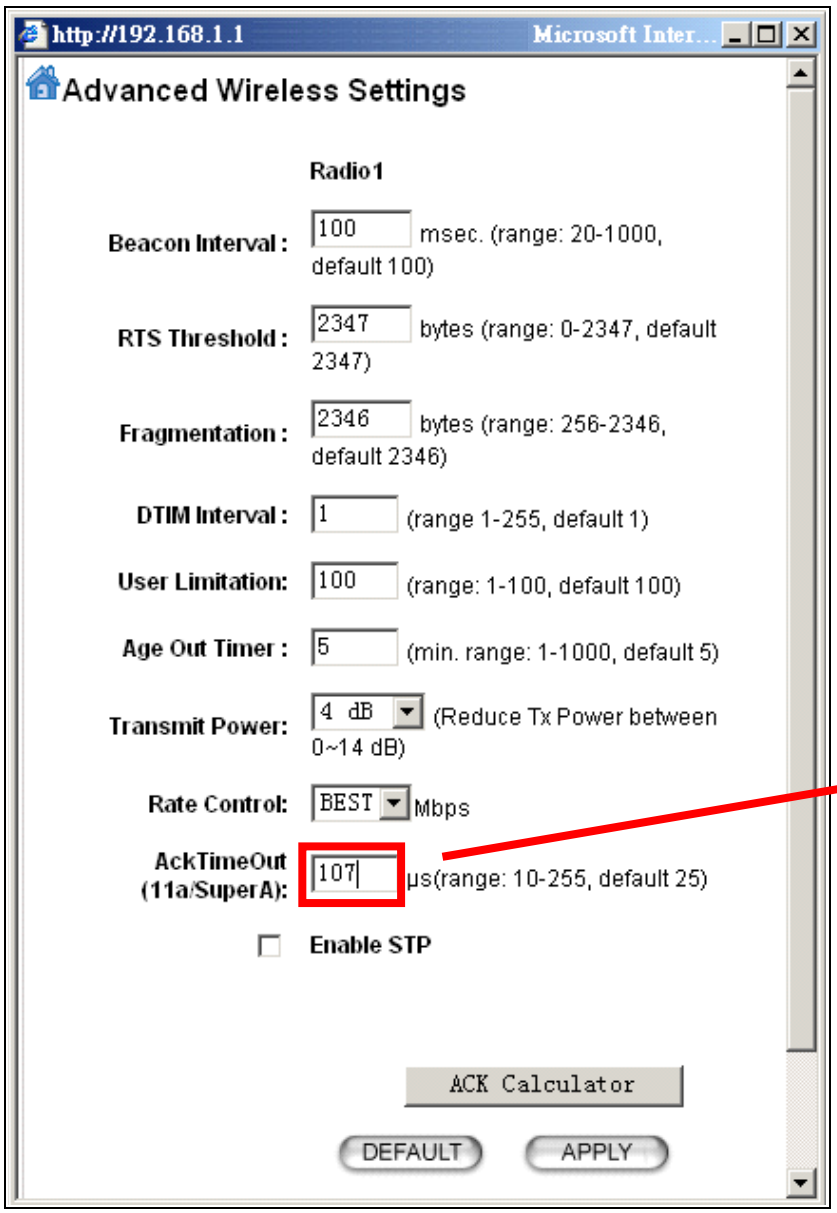


In the field of **“Distance”**, input the distance in **“meters”**.

After input the distance value, move the cursor to any place on the pop-up window out of three fields. The calculated value will display.



Enter the calculated value of **"AckTimeOut"** into the appropriate **"Ack TimeOut"** field (11a or 11g) in the **"Advanced Wireless Settings"** window.



Change the value from 25 to 107, where 107 is calculated value of distanced 12500m.

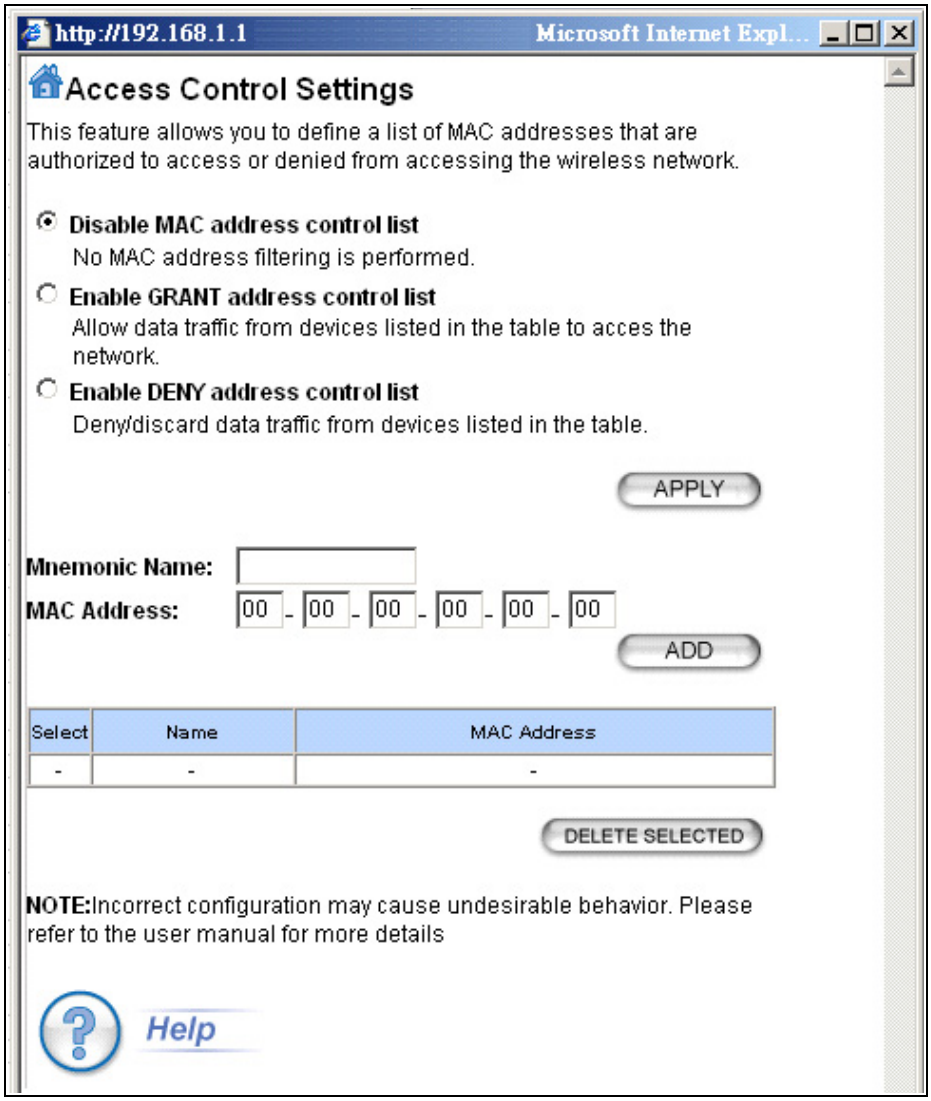
3.8 Access Control

The WH-9200AP allows you to define a list of MAC addresses that are allowed or denied to access the wireless network. Click on the setup button of "Access Control" of selected wireless interface.

Disable MAC address control list: When selected, no MAC address filtering will be performed.

Enable GRANT address control list: When selected, data traffic from only the specified devices in the table will be allowed in the network.

Enable DENY address control list: When selected, data traffic from the devices specified in the table will be denied/discarded by the network.



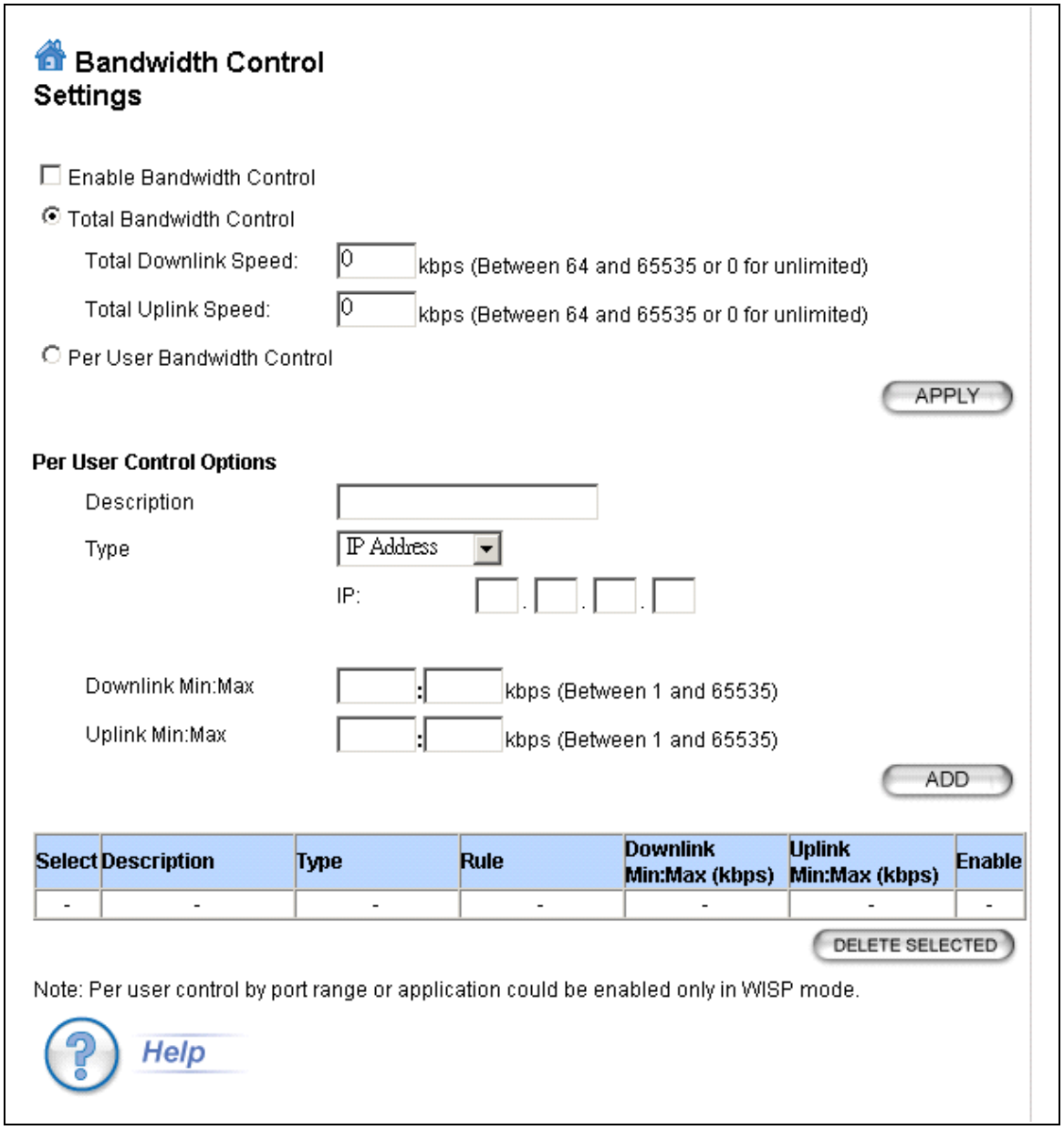
To add a MAC address into the table, enter a Mnemonic Name and the MAC Address, and then click ADD. The table lists all configured MAC Filter entries.

To delete entries, check the corresponding Select boxes and then press DELETE SELECTED.

3.9 Bandwidth Control

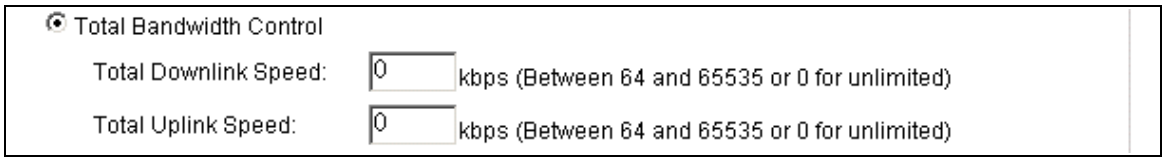
Bandwidth Control is a great tool to control the bandwidth of the WISP subscribers. Therefore, the WISP operators can offer different class of connection speeds for different subscription fees - just like the ADSL service! The AirLive advance firmware can control the bandwidth by Interface or IP/MAC.

There are 2 types of Traffic Control it offers: Total bandwidth control and Per-use bandwidth control.



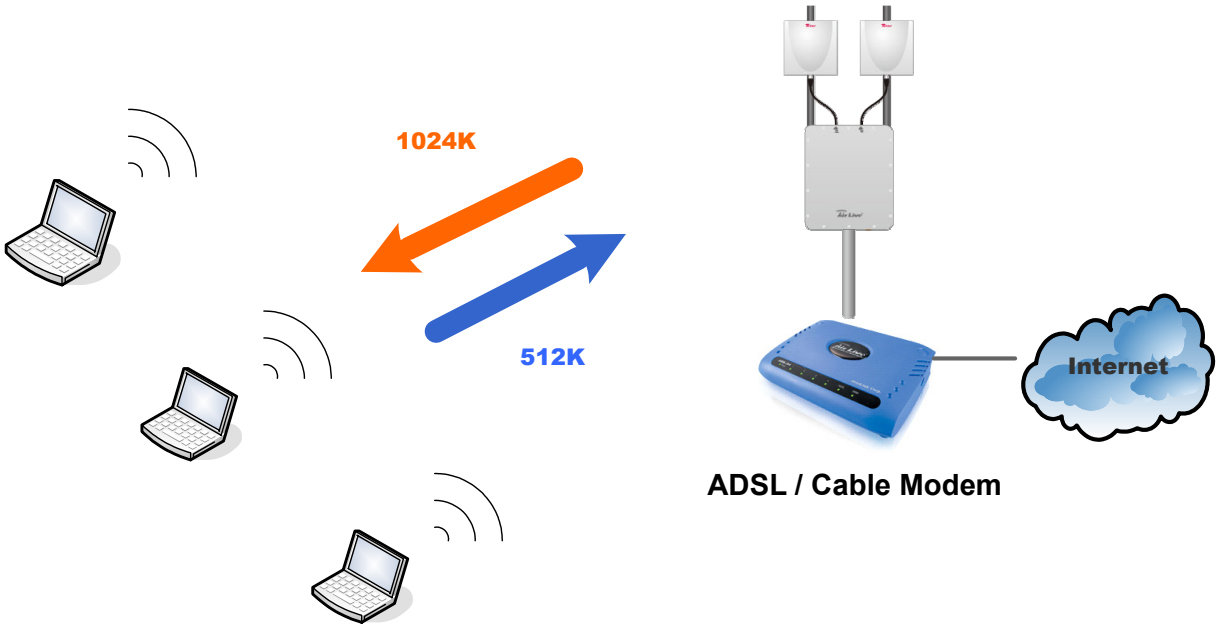
3.9.1 Total Bandwidth Control

The total bandwidth controls the data rate at either Wired or Wireless interface.



The following example limit the download bandwidth to **1024kbps** and uplink to **512kbps**

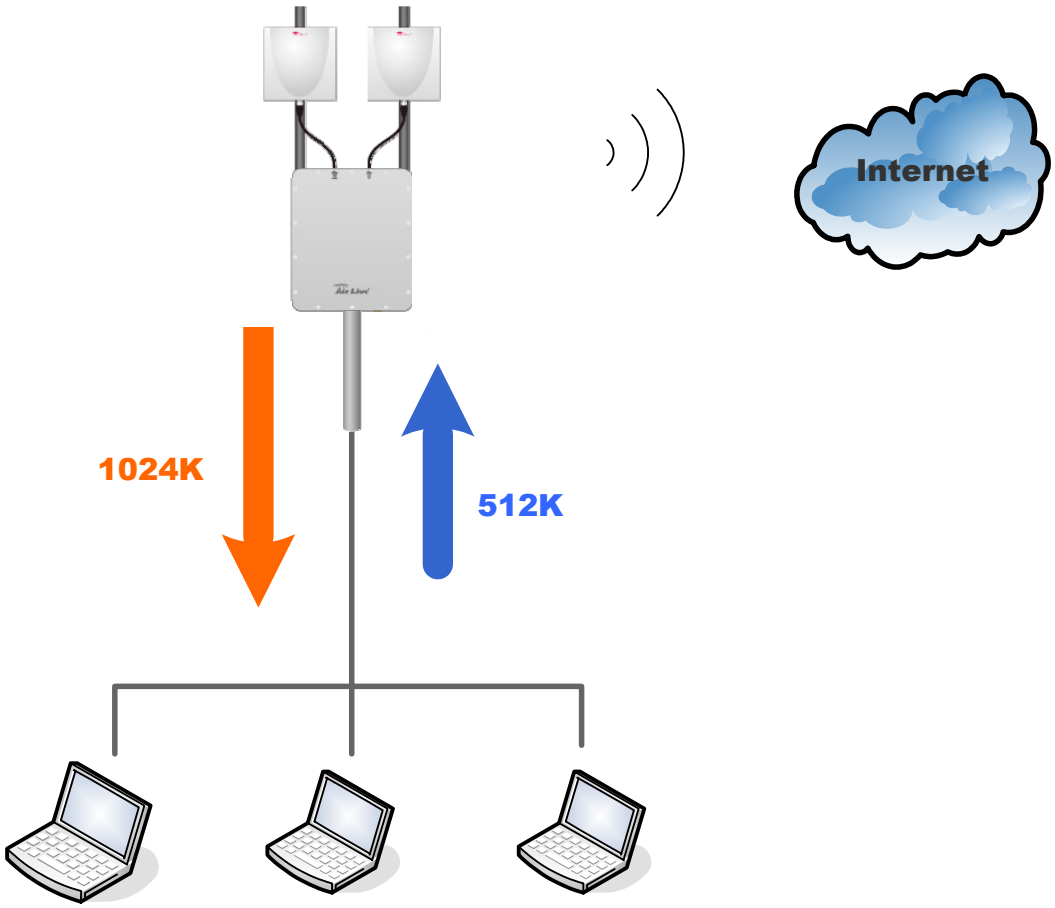
Example1: 3 wireless clients share downlink and uplink bandwidth.



In this example, total uplink bandwidth of the 3 clients is limited to 512kbps and the total download bandwidth of the 3 clients is limited to 1024kbps.

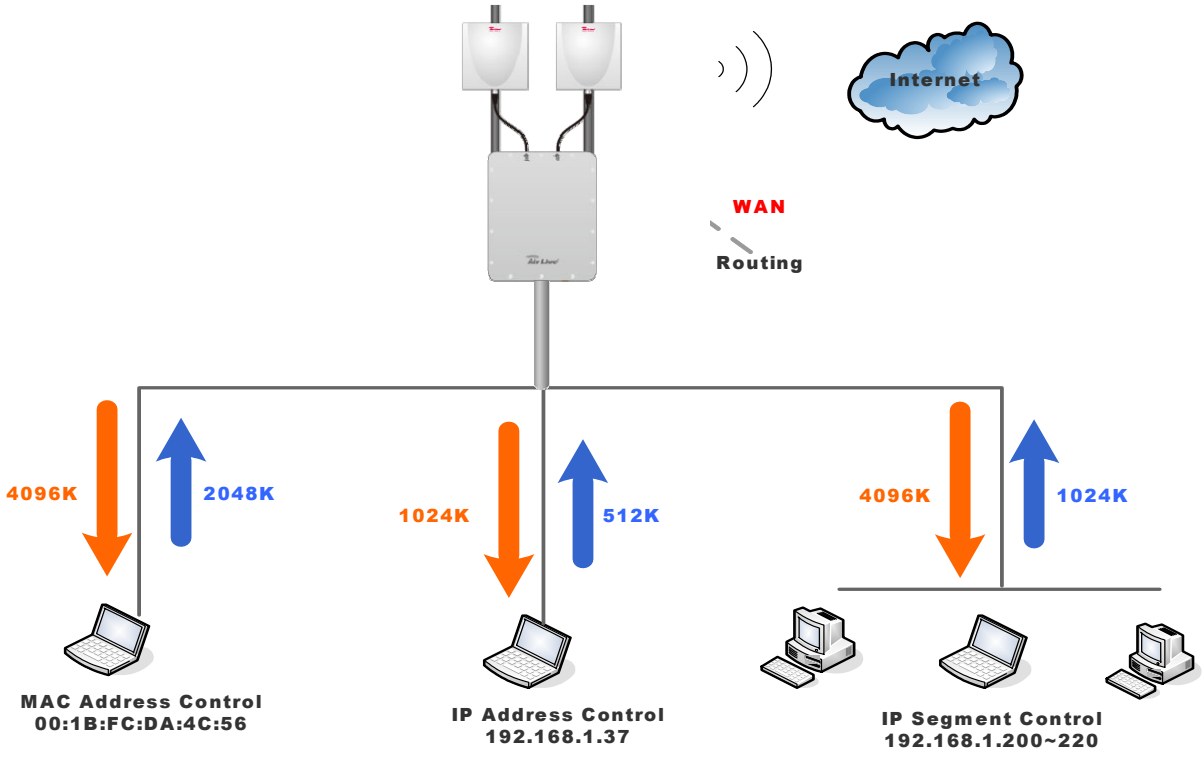
Example2:

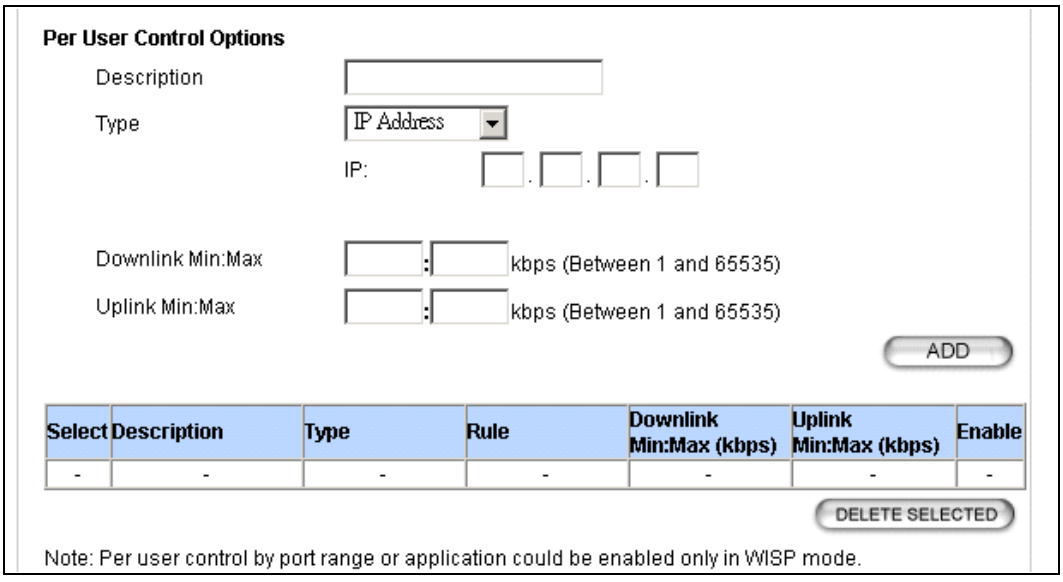
3 wired clients share downlink and uplink bandwidth.



In this example, total uplink bandwidth of the 3 clients is limited to 512kbps and the total download bandwidth of the 3 clients is limited to 1024kbps.

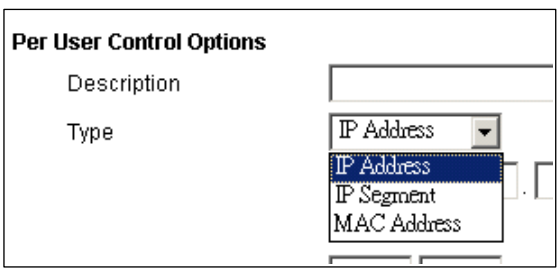
3.9.2 Per user Bandwidth Control





Note that this option could be enabled in WISP mode.

Description: You can preset your control type and named on the type.

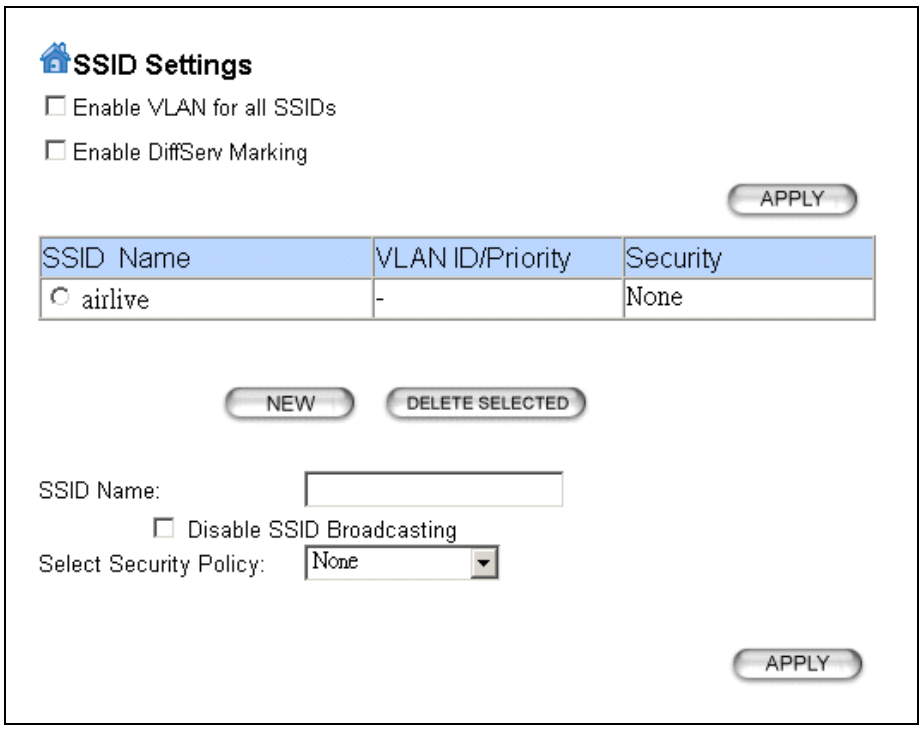


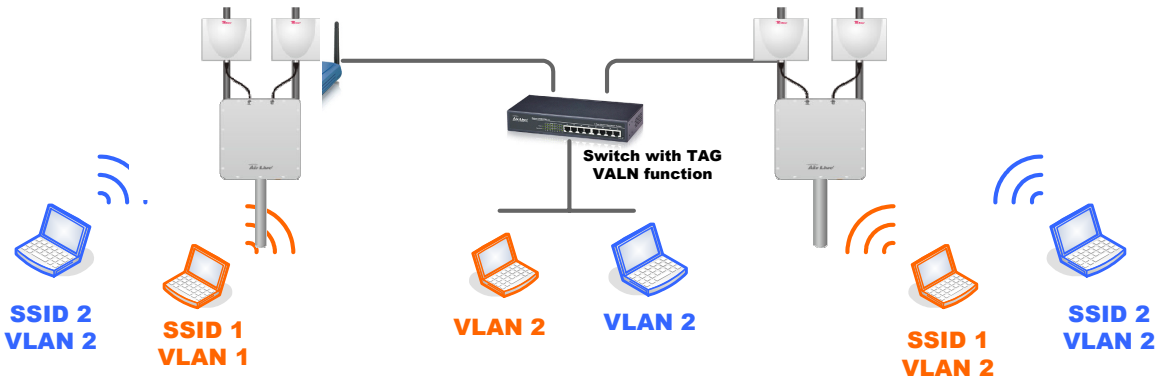
Type: Three types to be selected: IP Address, IP Segment and MAC Address. IP Segment allows you to set bandwidth limitation on an IP range.

3.10 Multiple SSID + VLAN

You can configure up to 4 SSIDs on your access point and assign different configuration settings to each SSID. All the SSIDs are active at the same time; that is, client devices can associate to the access point using any of the SSIDs. You can also assign VALN on each SSID to separate clients.

Note that the VLAN accept only tagged packet only.





In the above example, laptops in VALN 1 can only communicate with those in VLAN 1 and laptops in VALN 2 can only communicate with those in VLAN 2.

4 System Management

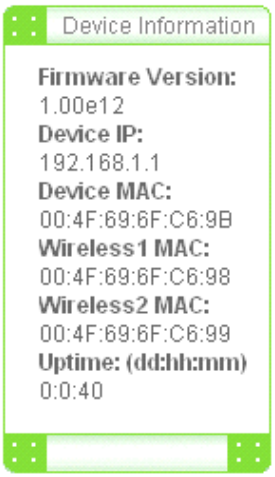
You can review the Device information of your WH-9200AP by the interface.

The information shows the current firmware version, IP address of your WH-9200AP.

Wireless1 MAC and **Wireless2 MAC** show the MAC address of the two radios, the information helps to setup WDS connection by remote access point.

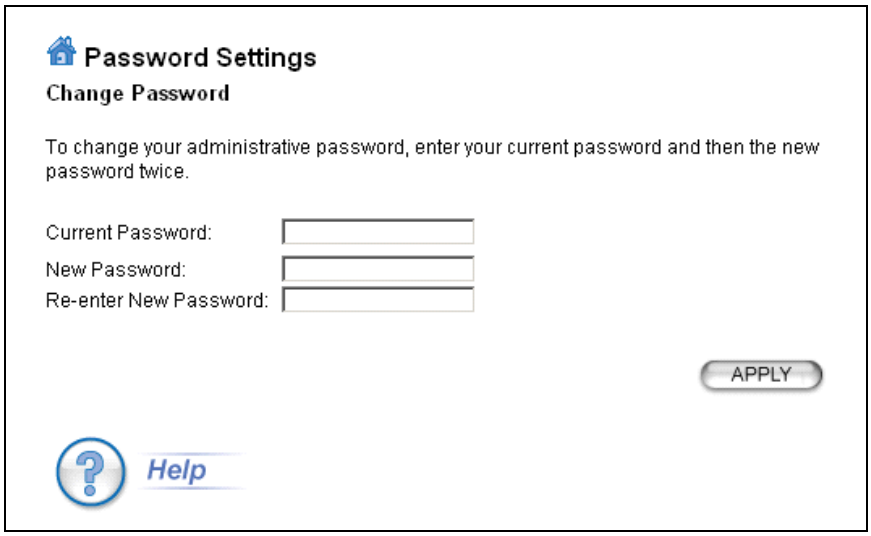
The **Uptime** records the live time of WH-9200AP after boot.

dd: day; **hh:** hour; **mm:** minute



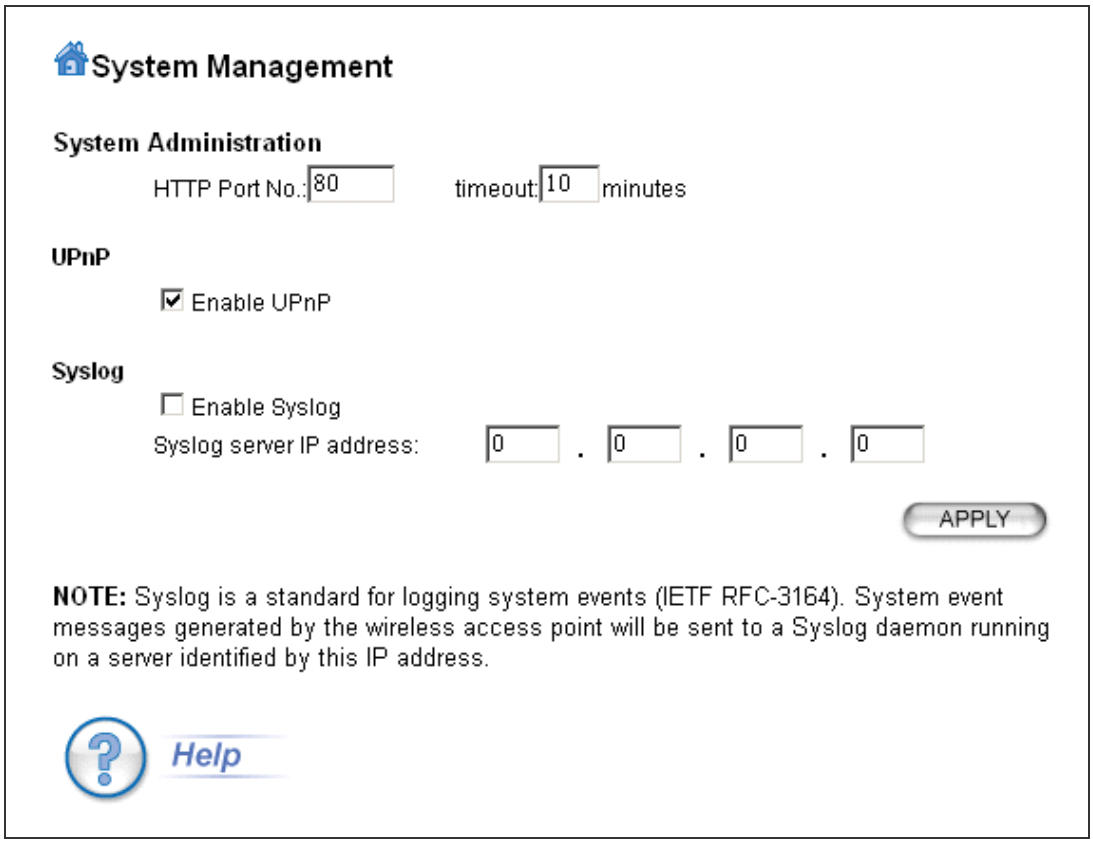
4.1 Change Password

It's recommended to set your own password instead of using default factory password. The default factory password is "**airlive**" all letters are in lower case. To change the password, press the **Password Settings** button to enter the **Password Settings** screen; then enter the Current Password followed by the New Password twice. The entered characters will appear as asterisks.



4.2 System Management Settings

The WH-9200AP allow you to change the parameter of manage the system.



HTTP Port No.: This is to change the management web port of WH-9200AP. By default, the port number is 80 and we type http://192.168.1.1 in the browser to access the management web page. If we change the port to another, say, 90, then we need to type http://192.168.1.1:90 instead. This prevents unwelcome access to the management interface.

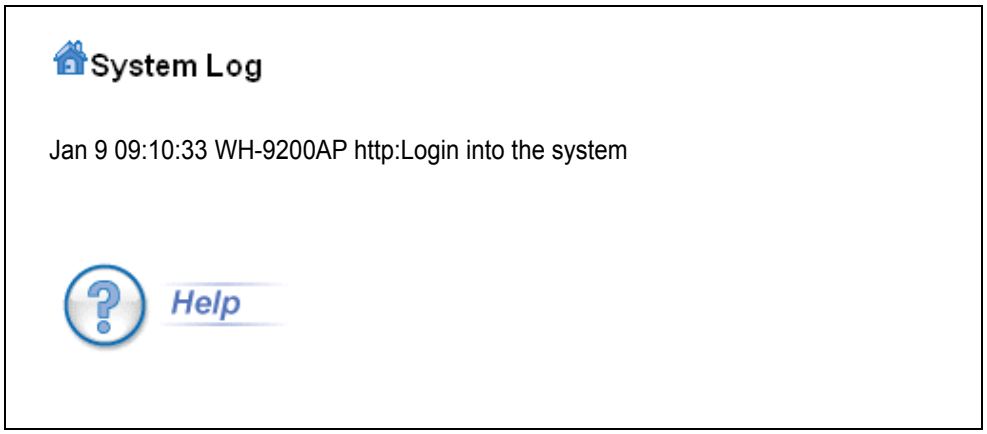
Time-out: The default is 10 minutes. If you idle on the web management interface more than 10 minutes, the system log you out and you need to login again.

UPnP: The Universal Plug and Play (UPnP) feature allows a Windows XP/ME PC to discover this WH-9200AP and automatically show an icon on the screen. Then a user can double-click the icon to access this device directly (without having to find out its IP address).

Syslog: If the Syslog is Enabled, WH-9200AP create a log in the system log table when encounters an error or warning condition. This apply to IETF (Internet Engineering Task Force - the Internet standards body)-conformant standard for logging system events (RFC-3164)

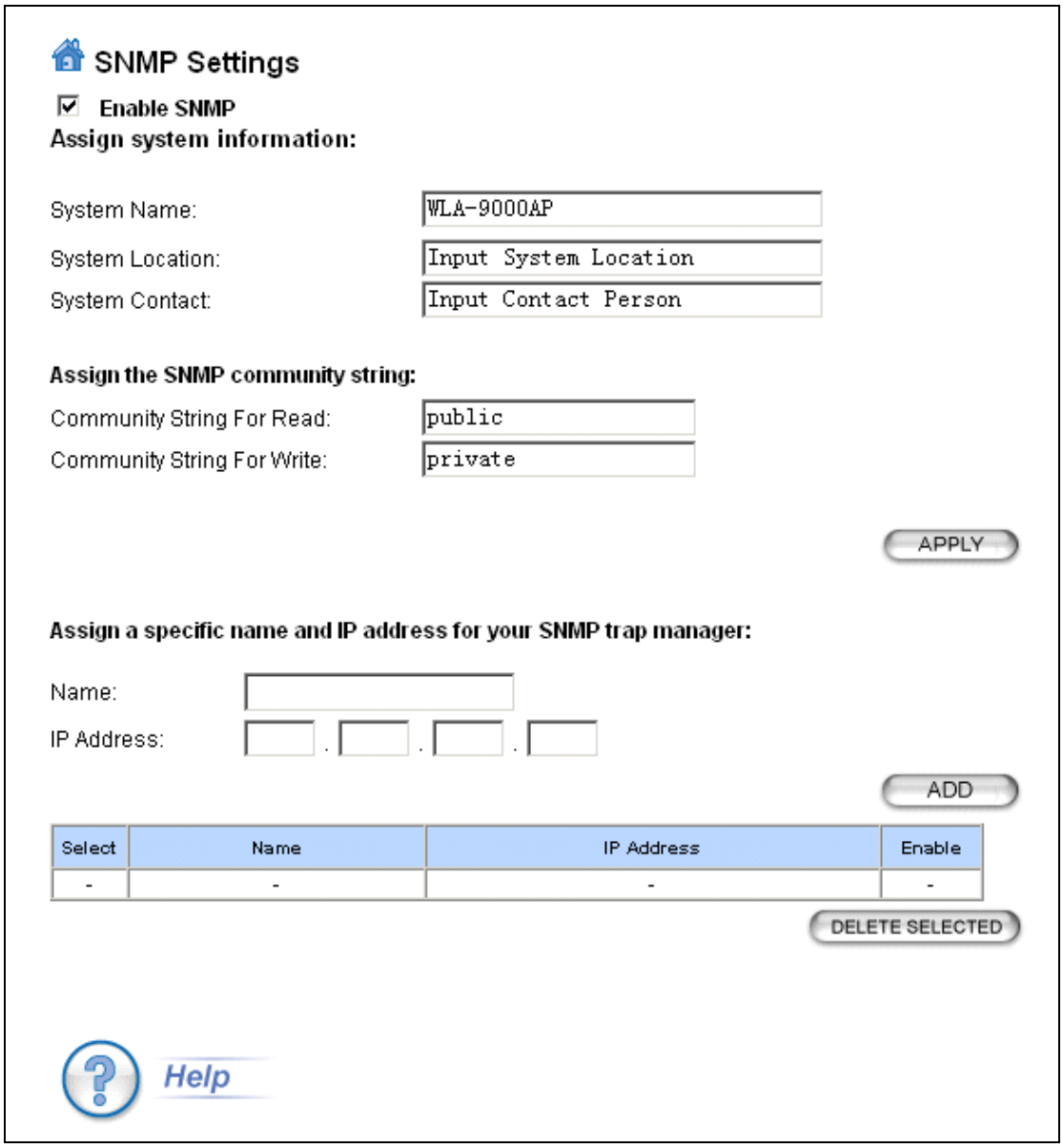
Syslog server IP address: The Syslog can also send to the identified IP address.

The system log shows in WH-9200AP:



4.3 SNMP Settings

WH-9200AP can also be managed by remote software with SNMP (simple network management protocol) protocol.



System Name: A name that you assign to your WH-9200AP for SNMP software. It is an alphanumeric string of up to 30 characters.

System Location: Enter a system location. Information for SNMP software.

System Contact: Contact information for the system administrator responsible for managing your WH-9200AP. It is an alphanumeric string of up to 60 characters.

Community String For Read: If you intend the router to be managed from a remote SNMP management station, you need to configure a read-only “community string” for read-only operation. The community string is an alphanumeric string of up to 15 characters.

Community String For Write: For read-write operation, you need to configure a write “community string”.

Assign a specific name and IP address for your SNMP trap manager:

A trap manager is a remote SNMP management station where special SNMP trap messages are generated (by the router) and sent to in the network.

You can define trap managers in the system.

You can add a trap manager by entering a **name**, an **IP address**, followed by pressing the **ADD** button.

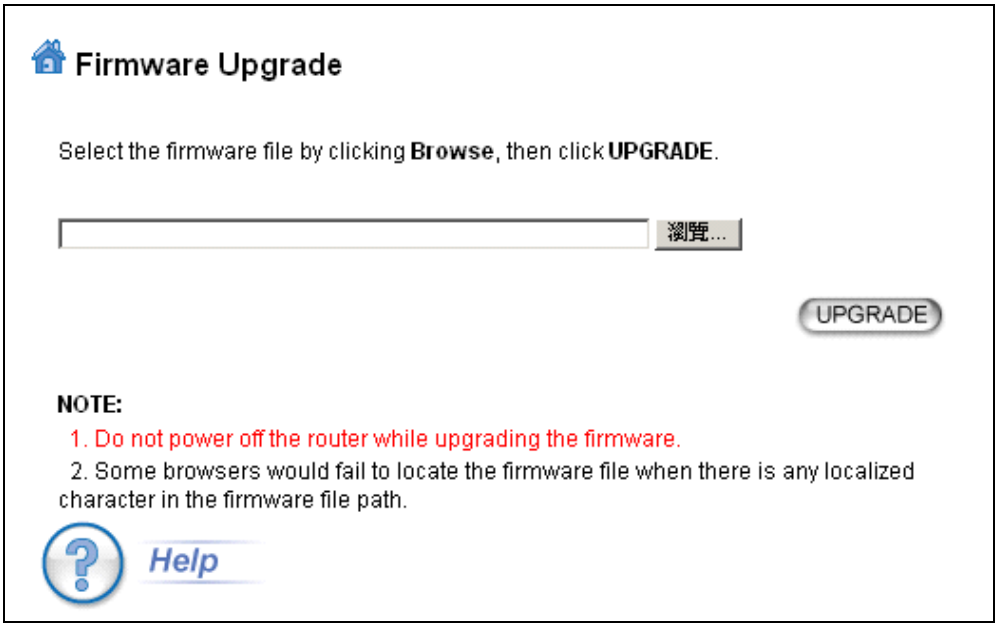
You can delete a trap manager by selecting the corresponding entry and press the **DELETE SELECTED** button.

To enable a trap manager, check the **Enable** box in the corresponding entry; to disable it, un-check the **Enable** box.

Some extra feature of WH-9200AP does not show in the wizard because some higher knowledge of parameters of them is required. They are classified in the tab of “Advances Setting”, such as the Multi SSID for VLAN setting and 802.11e QoS configuration.

4.4 Firmware Upgrade

You can upgrade the firmware of your WH-9200AP (the software that controls your WH-9200AP’s operation). Normally, this is done when a new version of firmware offers new features that you want, or solves problems that you have encountered with the current version. System upgrade can be performed through the System Upgrade window as follows:



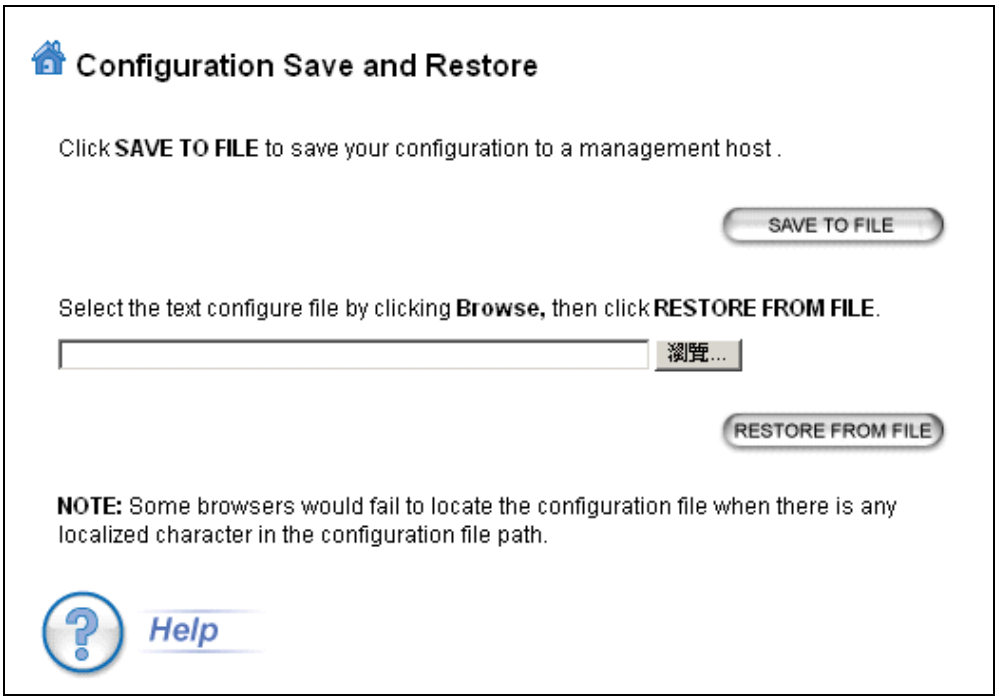
To update the WH-9200AP firmware, first download the firmware from the distributor's web site to your local disk, and then from the above screen enter the path and filename of the firmware file (or click **Browse** to locate the firmware file). Next, Click the **Upgrade** button to start.

The new firmware will be loaded to your WH-9200AP. After a message appears telling you that the operation is completed, you need to reset the system to have the new firmware take effect.

Do not power off the device while upgrading the firmware.
It is recommended that you do not upgrade your WH-9200AP unless the new firmware has new features you need or if it has a fix to a problem that you've encountered.

4.5 Configuration Save and Restore

In this interface, you can backup your system configuration to PC and restore your saved configuration file to the WH-9200AP.



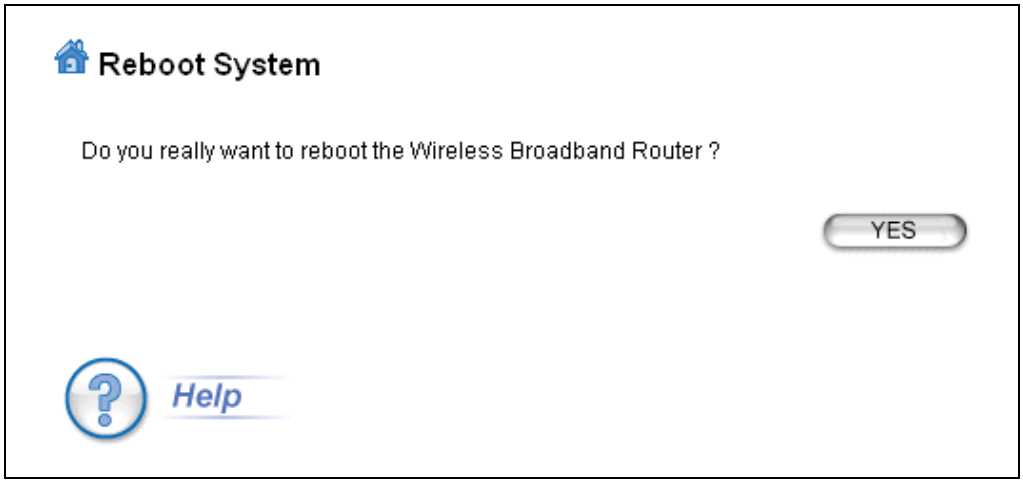
To save the configuration to your PC, click the **"SAVE TO FILE"** button and the system will

lead you to save the configuration file to your PC.

To restore configure file to WH-9200AP, click the **"Browse"** button, find the saved configuration fire, then click **"RESTORE FROM FILE"** button to restore.

4.6 Reboot System

The following interface allows you to reboot your WH-9200AP. Click **"Yes"** button to reboot.

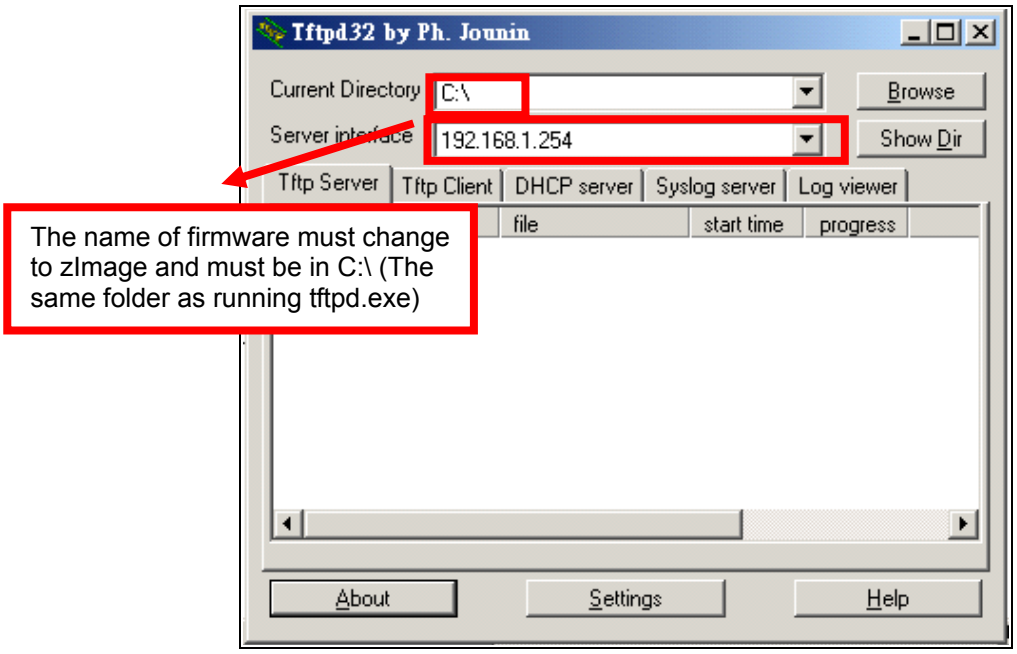


You can also reboot WH-9200AP by power off and power on it.

4.7 WH-9200AP Emergency Recovery

This document guides to recover your WH-9200AP system if the firmware crashed.

1. Download the tftp server to your PC. In the following example, we use tftpd32: http://tftpd32.jounin.net/tftpd32_download.html.
2. Copy the tftpd32.exe of the downloaded file to C:\.
3. Change the IP address of your PC to 192.168.1.254 / 255.255.255.0
4. Copy the WH-9200AP firmware to C:\ and rename the firmware to **"zImage"**. Note that the name must be zImage and no extension.
5. Connect WH-9200AP and PC with an Ethernet cable.
6. Run the tftpd32.exe. Note that the IP address must be 192.168.1.254.



7. Power on WH-9200AP, the **"Status"** LED will light on after 3 seconds.
8. Push the **"Reset"** button until the **"Status"** LED off and on again and release the **"Reset"** button.
9. If the above process success, the WH-9200AP LAN LED keep flashing and the tftp serve shows file download information.
10. It takes around 5 minutes to download firmware and around 5 minutes to update the firmware.
11. After a successful recovery, the WH-9200AP boots up automatically.
12. Try access 192.168.1.1, or the IP address you had changed before.

Repeat the processes again if failed.

5 Specifications

The specification of WH-9200AP is subject to change without notice. Please use the information with caution.

Feature

- 1 x 108Mbps 11a Radio + 1 x 108Mbps 11a/b/g Radio
- Atheros Super A and Super G Support
- High Output Power in 11a(23dB) and 11g/b Mode(23dB in America, 20dB in EU)
- Up to 14 Wireless Operation Modes
- 2 LAN Ports
- 2 N-Type Antenna connectors
- WDS Site Survey and RSSI Signal Survey
- Multi-SSID, VLAN, SNMP
- Bandwidth Control, TOS, and WMM
- Wireless user limitation

Hardware

- 220MHz Atheros CPU
- High power design , 23dBm average power, to extend the wireless range
- Dual wireless interface 11a, 11a/b/g + 11a, operation simultaneously.
- Super A/G mode support (Atheros Proprietary)
- RoHS compliant
- IEEE 802.3af (PoE) compliance
- 8MB Flash, 32MB SDRAM
- PoE support by one LAN port
- IP-67 Water Proof Metal Housing

Antenna

- 2 x N-Type antenna connectors

Frequency Range

- WLAN1(Radio 1)
  - 802.11a : 5.15 to 5.825 GHz
- WLAN2 (Radio 2)
  - 802.11b/g : 2.412 to 2.472 GHz
  - 802.11a : 5.15 to 5.825 GHz

Frequency Channel

- WLAN1(Radio 1)
  - 802.11a
    - USA (FCC) : 12
    - Europe (ETSI) : 19
- - WLAN2(Radio 2)
  - 802.11b/g
    - USA (FCC) : 11
    - Europe (ETSI) : 13
  - 802.11a
    - USA (FCC) : 12
    - Europe (ETSI) : 19

Power Supply

- 48V/0.4A Power Over Ethernet Adapter

Modulation Technology

- IEEE802.11a 5GHz OFDM
- IEEE802.11b 2.4GHz CCK
- IEEE802.11g 2.4GHz OFDM
- Atheros Proprietary Super A/G mode 802.11a Orthogonal

Wireless transfer Data Rate with Automatic Fallback

- 802.11b: 1, 2, 5.5, 11Mbps
- 802.11g: 1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54Mbps
- 802.11a: 6, 9, 12, 18, 24, 36, 48, 54Mbps

Output Power

802.11a	802.11g
54 Mbps @ 17dBm	54 Mbps @ 19dBm
48 Mbps @ 18dBm	48 Mbps @ 20dBm
36 Mbps @ 19 dBm	36 Mbps @ 21 dBm
6, 9, 12, 18, 24 Mbps @ 23 dBm	6, 9, 12, 18, 24 Mbps @ 23 dBm

RSSI

802.11a	802.11g
6Mbps @ -90 dBm	6Mbps @ -89 dBm
9Mbps @ -89 dBm	9Mbps @ -88 dBm
12Mbps @ -88 dBm	12Mbps @ -88 dBm
18Mbps @ -86 dBm	18Mbps @ -86 dBm
24Mbps @ -82 dBm	24Mbps @ -82 dBm
36Mbps @ -79 dBm	36Mbps @ -79 dBm
48Mbps @ -73 dBm	48Mbps @ -75 dBm
54Mbps @ -71 dBm	54Mbps @ -73 dBm

Software

- Wi-Fi, WPA compatible interoperability
- Support WDS Bridge Mode, Client Mode, AP Mode on interface under each predefined operational mode
- Client Isolation supported
- SNMP v1/v2 support
- Support adjustable output power
- ACK Timeout setting
- User Limitation (Static Load Balancing)
- Multiple SSID, VLAN, QoSWPA with PSK/TKIP/AES support ,WPA2 support
- 152-bit WEP support (Atheros Proprietary)
- Super A/G mode support (Atheros Proprietary)

- Bootloader Protection and Emergency Firmware Upload Code in bootloader
- Radius Support
- HTB QoS
- P2P Bandwidth Control

Product Weight (g)

- 1105 g

Product Size (L x W x H mm)

- 225 x 122 x 225 mm

6 Wireless Network Glossary

The wireless network glossary contains explanation or information about common terms used in wireless networking products. Some of information in this glossary might be outdated, please use with caution.

802.11a
An IEEE specification for wireless networking that operates in the 5 GHz frequency range (5.15 GHz to 5.850 GHz) with a maximum of 54 Mbps data transfer rate. The 5 GHz frequency band is not as crowded as the 2.4 GHz band. In addition, the 802.11a have 12 non-overlapping channels, comparing to 802.11b/g's 3 non-overlapping channels. This means the possibility to build larger non-interfering networks. However, the 802.11a deliver shorter distance at the same output power when comparing to 802.11g.

802.3ad
802.3ad is an IEEE standard for bonding or aggregating multiple Ethernet ports into one virtual port (also known as trunking) to increase the bandwidth.

802.3af
This is the PoE (Power over Ethernet) standard by IEEE committee. 803.af uses 48V POE standard that can deliver up to 100 meter distance over Ethernet cable.

802.11b
International standard for wireless networking that operates in the 2.4 GHz frequency band (2.4 GHz to 2.4835 GHz) and provides a throughput up to 11 Mbps.

802.1d STP
Spanning Tree Protocol. It is an algorithm to prevent network from forming. The STP protocol allows net work to provide a redundant link in the event of a link failure. It is advise to turn on this option for multi-link bridge network.

802.11d
Also known as “Global Roaming”. 802.11d is a standard for use in countries where systems using other standards in the 802.11 family are not allowed to operate.

802.11e
The IEEE QoS standard for prioritizing traffic of the VoIP and multimedia applications. The WMM is based on a subset of the 802.11e.

802.11g
A standard provides a throughput up to 54 Mbps using OFDM technology. It also operates in the 2.4 GHz frequency band as 802.11b. 802.11g devices are backward compatible with 802.11b devices.

802.11h
This IEEE standard define the TPC (transmission power control) and DFS(dynamic frequency selection) required to operate WiFi devices in 5GHz for EU.

802.11i
The IEEE standard for wireless security. 802.11i standard includes TKIP, CCMP, and AES encryption to improve wireless security. It is also know as WPA2.

802.1Q Tag VLAN
In 802.1Q VLAN, the VLAN information is written into the Ethernet packet itself. Each packet carries a VLAN ID(called Tag) as it traveled across the network. Therefore, the VLAN configuration can be configured across multiple switches. In 802.1Q spec, possible 4096 VLAN ID can be created. Although for some devices, they can only view in frames of 256 ID at a time.

802.1x
802.1x is a security standard for wired and wireless LANs. In the 802.1x parlance, there are usually supplicants (client), authenticator (switch or AP), and authentication server (radius server) in the network. When a supplicants request a service, the authenticator will pass the request and wait for the authentication server to grant access and register accounting. The 802.1x is the most widely used method of authentication by WISP.

Adhoc

A Peer-to-Peer wireless network. An Adhoc wireless network do not use wireless AP or router as the central hub of the network. Instead, wireless client are connected directly to each other. The disadvantage of Adhoc network is the lack of wired interface to Internet connections. It is not recommended for network more than 2 nodes.

Access Point (AP)

The central hub of a wireless LAN network. Access Points have one or more Ethernet ports that can connect devices (such as Internet connection) for sharing. Multi-function Access Point can also function as an Ethernet client, wireless bridge, or repeat signals from other AP. Access Points typically have more wireless functions comparing to wireless routers.

ACK Timeout

Acknowledgement Timeout Windows. When a packet is sent out from one wireless station to the other, it will waits for an Acknowledgement frame from the remote station. The station will only wait for a certain amount of time, this time is called the ACK timeout. If the ACK is NOT received within that timeout period then the packet will be re-transmitted resulting in reduced throughput. If the ACK setting is too high then throughput will be lost due to waiting for the Ack Window to timeout on lost packets. If the ACK setting is too low then the ACK window will have expired and the returning packet will be dropped, greatly lowering throughput. By having the ability to adjust the ACK setting we can effectively optimize the throughput over long distance links. This is especially true for 802.11a and 802.11g networks. Setting the correct ACK timeout value needs to consider 3 factors: distance, AP response time, and interference. The WH-9200AP provides ACK adjustment capability in form of either distance or direct input. When you enter the distance parameter, the WH-9200AP will automatically calculate the correct ACK timeout value.

Bandwidth Management

Bandwidth Management controls the transmission speed of a port, user, IP address, and application. Router can use bandwidth control to limit the Internet connection speed of individual IP or Application. It can also guarantee the speed of certain special application or privileged IP address - a crucial feature of QoS (Quality of Service) function. The WH-9200AP's features both "Per-user Bandwidth Control" and "Total Bandwidth Control". "Per-user Bandwidth Control" allow administrator to define the maximum bandwidth of each user by IP, IP Group, or MAC address. Total Bandwidth defines the maximum bandwidth of wireless or Ethernet interface.

Bootloader
Bootloader is the under layering program that will start at the power-up before the device loads firmware. It is similar to BIOS on a personal computer. When a firmware crashed, you might be able to recover your device from bootloader.

Bridge
A product that connects 2 different networks that uses the same protocol. Wireless bridges are commonly used to link network across remote buildings. For wireless application, there are 2 types of Bridges. WDS Bridge can be used in Point-to-Point or Point-to-Multipoint topology. Bridge Infrastructure works with AP mode to form a star topology.

Cable and Connector Loss: During wireless design and deployment, it is important to factor in the cable and connector loss. Cable and connector loss will reduce the output power and receiver sensitivity of the radio at connector end. The longer the cable length is, the more the cable loss. Cable loss should be subtracted from the total output power during distance calculation. For example, if the cable and connector loss is 3dBm and the output power is 20dBm; the output power at the cable end is only 17dBm.

Client
Client means a network device or utility that receives service from host or server. A client device means end user device such as wireless cards or wireless CPE.

CPE Devices
CPE stands for Customer Premises Equipment. A CPE is a device installed on the end user's side to receive network services. For example, on an ADSL network, the ADSL modem/router on the subscriber's home is the CPE device. Wireless CPE means a complete Wireless (usually an AP with built-in Antenna) that receive wireless broadband access from the WISP. The opposite of CPE is CO.

CTS
Clear To Send. A signal sent by a device to indicate that it is ready to receive data.

DDNS
Dynamic Domain Name System. An algorithm that allows the use of dynamic IP address

for hosting Internet Server. A DDNS service provides each user account with a domain name. A router with DDNS capability has a built-in DDNS client that updates the IP address information to DDNS service provider whenever there is a change. Therefore, users can build website or other Internet servers even if they don't have fixed IP connection.

DHCP

Dynamic Hosting Configuration Protocol. A protocol that enables a server to dynamically assign IP addresses. When DHCP is used, whenever a computer logs onto the network, it automatically gets an IP address assigned to it by DHCP server. A DHCP server can either be a designated PC on the network or another network device, such as a router.

DMZ

Demilitarized Zone. When a router opens a DMZ port to an internal network device, it opens all the TCP/UDP service ports to this particular device. The feature is used commonly for setting up H.323 VoIP or Multi-Media servers.

DNS

A program that translates URLs to IP addresses by accessing a database maintained on a collection of Internet servers.

Domain Name

The unique name that identifies an Internet site. Domain Names always have 2 or more parts, separated by dots. In www.airlive.com, the "airlive.com" is the doman name.

DoS Attack

Denial of Service. A type of network attack that floods the network with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols.

Encryption

Encoding data to prevent it from being read by unauthorized people. The common wireless encryption schemes are WEP, WPA, and WPA2.

ESSID (SSID)
The identification name of an 802.11 wireless network. Since wireless network has no physical boundary liked wired Ethernet network, wireless LAN needs an identifier to distinguish one network from the other. Wireless clients must know the SSID in order to associate with a WLAN network. Hide SSID feature disable SSID broadcast, so users must know the correct SSID in order to join a wireless network.

Firewall
A system that secures a network and prevents access by unauthorized users. Firewalls can be software, router, or gateway. Firewalls can prevent unrestricted access into a network, as well as restricting data from flowing out of a network.

Firmware
The program that runs inside embedded device such as router or AP. Many network devices are firmware upgradeable through web interface or utility program.

FTP
File Transfer Protocol. A standard protocol for sending files between computers over a TCP/IP network and the Internet.

Fragment Threshold
Frame Size larger than this will be divided into smaller fragment. If there are interferences in your area, lower this value can improve the performance. If there are not, keep this parameter at higher value. The default size is 2346. You can try 1500, 1000, or 500 when there are interference around your network.

Full Duplex
The ability of a networking device to receive and transmit data simultaneously. In wireless environment, this is usually done with 2 or more radios doing load balancing.

Gateway
In the global Internet network, the gateways are core routers that connect networks in different IP subnet together. In a LAN environment with an IP sharing router, the gateway is the router. In an office environment, gateway typically is a multi-function device that integrates NAT, firewall, bandwidth management, and other security functions.

Hotspot
A place where you can access Wi-Fi service. The term hotspot has two meanings in wireless deployment. One is the wireless infrastructure deployment, the other is the Internet access billing system. In a hotspot system, a service provider typically need an authentication and account system for billing purposes, and a wireless AP network to provide access for customers.

IGMP Snooping
Internet Group Management Protocol (IGMP) is a Layer 3 protocol to report IP multicast memberships to neighboring multicast switches and routers. IGMP snooping is a feature that allows an Ethernet switch to "listen in" on the IGMP conversation between hosts and routers. A switch support IGMP snooping has the possibility to avoid multicast traffic being treated as broadcast traffic; therefore, reducing the overall traffic on the network.

Infrastructure Mode
A wireless network that is built around one or more access points to provide wireless clients access to wired LAN / Internet service. The opposite of Infrastructure mode is Adhoc mode.

IP address
IP (Internet Protocol) is a layer-3 network protocol that is the basis of all Internet communication. An IP address is 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: an identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network. The new IPv6 specification supports 128-bit IP address format.

IPsec
IP Security. A set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs). IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet.

LACP (802.3ad) Trunking

The 802.3ad Link Aggregation standard defines how to combine the several Ethernet ports into one high-bandwidth port to increase the transmission speed. It is also known as port trunking. Both device must set the trunking feature to work.

MAC
Media Access Control. MAC address provides layer-2 identification for Networking Devices. Each Ethernet device has its own unique address. The first 6 digits are unique for each manufacturer. When a network device have MAC access control feature, only the devices with the approved MAC address can connect with the network.

Mbps
Megabits Per Second. One million bits per second; a unit of measurement for data transmission

MESH
Mesh is an outdoor wireless technology that uses Spanning Tree Protocol (STP) and Wireless Distribution system to achieve self-forming, self-healing, and self-configuring outdoor network. MESH network are able to take the shortest path to a destination that does not have to be in the line of site.

MIMO
Multi In Multi Out. A Smart Antenna technology designed to increase the coverage and performance of a WLAN network. In a MIMO device, 2 or more antennas are used to increase the receiver sensitivity and to focus available power at intended Rx.

NAT
Network Address Translation. A network algorithm used by Routers to enables several PCs to share single IP address provided by the ISP. The IP that a router gets from the ISP side is called Real IP, the IP assigned to PC under the NAT environment is called Private IP.

Node
A network connection end point, typically a computer.

Packet
A unit of data sent over a network.

Passphrase
Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for the company products.

POE
Power over Ethernet. A standard to deliver both power and data through one single Ethernet cable (UTP/STP). It allows network device to be installed far away from power ource. A POE system typically compose of 2 main component: DC Injector (Base Unit) and Splitter(Terminal Unit). The DC injector combines the power and data, and the splitter separates the data and power back. A PoE Access Point or CPE has the splitter built-in to the device. The IEEE 802.3af is a POE spec that uses 48 volt to deliver power up to 100 meter distance.

Port
This word has 2 different meaning for networking.
- The hardware connection point on a computer or networking device used for plugging in a cable or an adapter.
- The virtual connection point through which a computer uses a specific application on a server.

PPPoE
Point-to- Point Protocol over Ethernet. PPPoE relies on two widely accepted standards: PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem.

PPTP
Point-to-Point Tunneling Protocol: A VPN protocol developed by PPTP Forum. With PPTP, users can dial in to their corporate network via the Internet. If users require data encryption when using the Windows PPTP client, the remote VPN server must support MPPE (Microsoft Point-To-Point Encryption Protocol) encryption. PPTP is also used by some ISP for user authentication, particularly when pairing with legacy Alcatel / Thomson ADSL modem.

Preamble Type
Preamble are sent with each wireless packet transmit for transmission status. Use the long preamble type for better compatibility. Use the short preamble type for better performance

Rate Control
Ethernet switches' function to control the upstream and downstream speed of an individual port. Rate Control management uses "Flow Control" to limit the speed of a port. Therefore, the Ethernet adapter must also have the flow control enabled. One way to force the adapter's flow control on is to set a port to half-duplex mode.

RADIUS
Remote Authentication Dial-In User Service. An authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP, you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system. Radius typically uses port 1812 and port 1813 for authentication and accounting port. Though not an official standard, the RADIUS specification is maintained by a working group of the IETF.

Receiver Sensitivity
Receiver sensitivity means how sensitive is the radio for receiving signal. In general; the slower the transmission speed, the more sensitive the radio is. The unit for Receiver Sensitivity is in dB; the lower the absolute value is, the higher the signal strength. For example, -50dB is higher than -80dB.

RJ-45
Standard connectors for Twisted Pair copper cable used in Ethernet networks. Although they look similar to standard RJ-11 telephone connectors, RJ-45 connectors can have up to eight wires, whereas telephone connectors have only four.

Router
An IP sharing router is a device that allows multiple PCs to share one single broadband connection using NAT technology. A wireless router is a device that combines the

functions of wireless Access Point and the IP sharing router.

RSSI
Receiver Sensitivity Index. RSSI is a value to show the Receiver Sensitivity of the remote wireless device. In general, remote APs with stronger signal will display higher RSSI values. For RSSI value, the smaller the absolute value is, the stronger the signal. For example, “-50db” has stronger signal than “-80dB”. For outdoor connection, signal stronger than -60dB is considered as a good connection.

RTS
Request To Send. A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data.

RTS Threshold
RTS (Request to Send). The RTS/CTS(clear to send) packet will be send before a frame if the packet frame is larger than this value. Lower this value can improve the performance if there are many clients in your network. You can try 1500, 1000 or 500 when there are many clients in your AP’s network.

SNMP
Simple Network Management Protocol. A set of protocols for managing complex networks. The SNMP network contains 3 key elements: managed devices, agents, and network-management systems (NMSs). Managed devices are network devices that content SNMP agents. SNMP agents are programs that reside SNMP capable device's firmware to provide SNMP configuration service. The NMS typically is a PC based software such as HP Openview that can view and manage SNMP network device remotely.

SSH
Developed by SSH Communications Security Ltd., Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist.

SSL
Secure Sockets Layer. It is a popular encryption scheme used by many online retail and banking sites to protect the financial integrity of transactions. When an SSL session

begins, the server sends its public key to the browser. The browser then sends a randomly generated secret key back to the server in order to have a secret key exchange for that session. SSL VPN is also known as Web VPN. The HTTPS and SSH management interface use SSL for data encryption.

Subnet Mask

An address code mask that determines the size of the network. An IP subnet are determined by performing a BIT-wise AND operation between the IP address and the subnet mask. By changing the subnet mask, you can change the scope and size of a network.

Subnetwork or Subnet

Found in larger networks, these smaller networks are used to simplify addressing between numerous computers. Subnets connect to the central network through a router, hub or gateway. Each individual wireless LAN will probably use the same subnet for all the local computers it talks to.

Super A

Super A is an Atheros proprietary turbo mode to increase speed over standard 802.11a mode. It adds Bursting and Compression to increase the speed. If you live in countries that prohibit the channel binding technology (i.e. Europe), you should choose “Super-A without Turbo) if you need more speed than 11a mode

TCP

A layer-4 protocol used along with the IP to send data between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the packets that a message is divided into for efficient routing through the Internet.

Turbo A

Turbo A is an Atheros proprietary turbo mode to increase speed over standard 802.11a mode. It uses channel binding technology to increase speed. There are 2 types of Turbo A modes: Dynamic Turbo and Static Turbo. In Dynamic Turbo, the channel binding will be used only if necessary. In Static Turbo, the channel binding is always on. This protocol may be combined with Super-A model to increase the performance even more. The used of channel binding might be prohibited in EU countries.

TX Output Power
Transmit Output Power. The TX output power means the transmission output power of the radio. Normally, the TX output power level limit for 2.4GHz 11g/b is 20dBm at the antenna end. The output power limit for 5GHz 802.11a is 30dBm at the antenna end..

UDP
User Datagram Protocol. A layer-4 network protocol for transmitting data that does not require acknowledgement from the recipient of the data.

Upgrade
To replace existing software or firmware with a newer version.

Upload
To send a file to the Internet or network device.

URL
Uniform Resource Locator. The address of a file located on the Internet.

VPN
Virtual Private Network. A type of technology designed to increase the security of information transferred over the Internet. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate network.

Walled Garden
On the Internet, a walled garden refers to a browsing environment that controls the information and Web sites the user is able to access. This is a popular method used by ISPs in order to keep the user navigating only specific areas of the Web

WAN
Wide Area Network. A communication system of connecting PCs and other computing devices across a large local, regional, national or international geographic area. A WAN

port on the network device means the port (or wireless connection) that is connected to the Internet side of the network topology.

WEP
Wired Equivalent Privacy. A wireless encryption protocol. WEP is available in 40-bit (64-bit), 108-bit (128-bit) or 152-bit (Atheros proprietary) encryption modes.

Wi-Fi
Wireless Fidelity. An interoperability certification for wireless local area network (LAN) products based on the IEEE 802.11 standards. The governing body for Wi-Fi is called Wi-Fi Alliance (also known as WECA).

WiMAX
Worldwide Interoperability for Microwave Access. A Wireless Metropolitan Network technology that complies with IEEE 802.16 and ETSI Hiperman standards. The orginal 802.16 standard call for operating frequency of 10 to 66Ghz spectrum. The 802.16a amendment extends the original standard into spectrum between 2 and 11 Ghz. 802.16d increase data rates to between 40 and 70 Mbps/s and add support for MIMO antennas, QoS, and multiple polling technologies. 802.16e adds mobility features, narrower bandwidth (a max of 5 mhz), slower speed and smaller antennas. Mobility is allowed up to 40 mph.

WDS
Wireless Distribution System. WDS defines how multiple wireless Access Point or Wireless Router can connect together to form one single wireless network without using wired uplinks. WDS associate each other by MAC address, each device

WLAN
Wireless Local Area Network. A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes. The most popular standard for WLAN is the 802.11 standards.

WMM
Wi-Fi Multimedia (WMM) is a standard to prioritize traffic for multimedia applications. The WMM prioritize traffic\ on Voice-over-IP (VoIP), audio, video, and streaming media as well

as traditional IP data over the AP.

WMS

Wireless Management System. An utility program to manage multiple wireless AP/Bridges.

WPA

Wi-Fi Protected Access. It is an encryption standard proposed by WiFi for advance protection by utilizing a password key (TKIP) or certificate. It is more secure than WEP encryption. The WPA-PSK utilizes pre-share key for encryption/authentication.

WPA2

Wi-Fi Protected Access 2. WPA2 is also known as 802.11i. It improves on the WPA security with CCMP and AES encryption. The WPA2 is backward compatible with WPA. WPA2-PSK utilizes pre-share key for encryption/authentication.